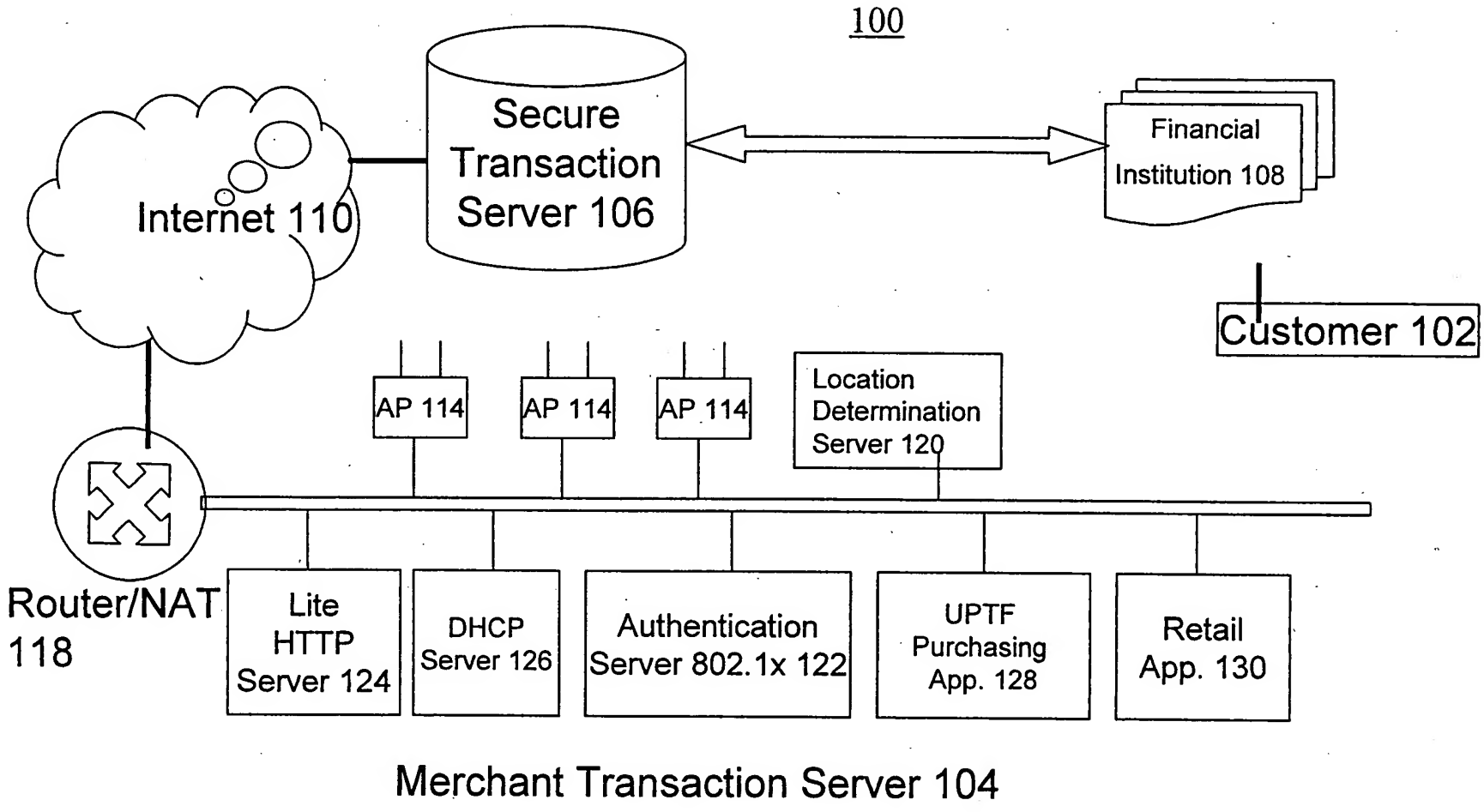


118, 120, 122 = optional

Figure 1

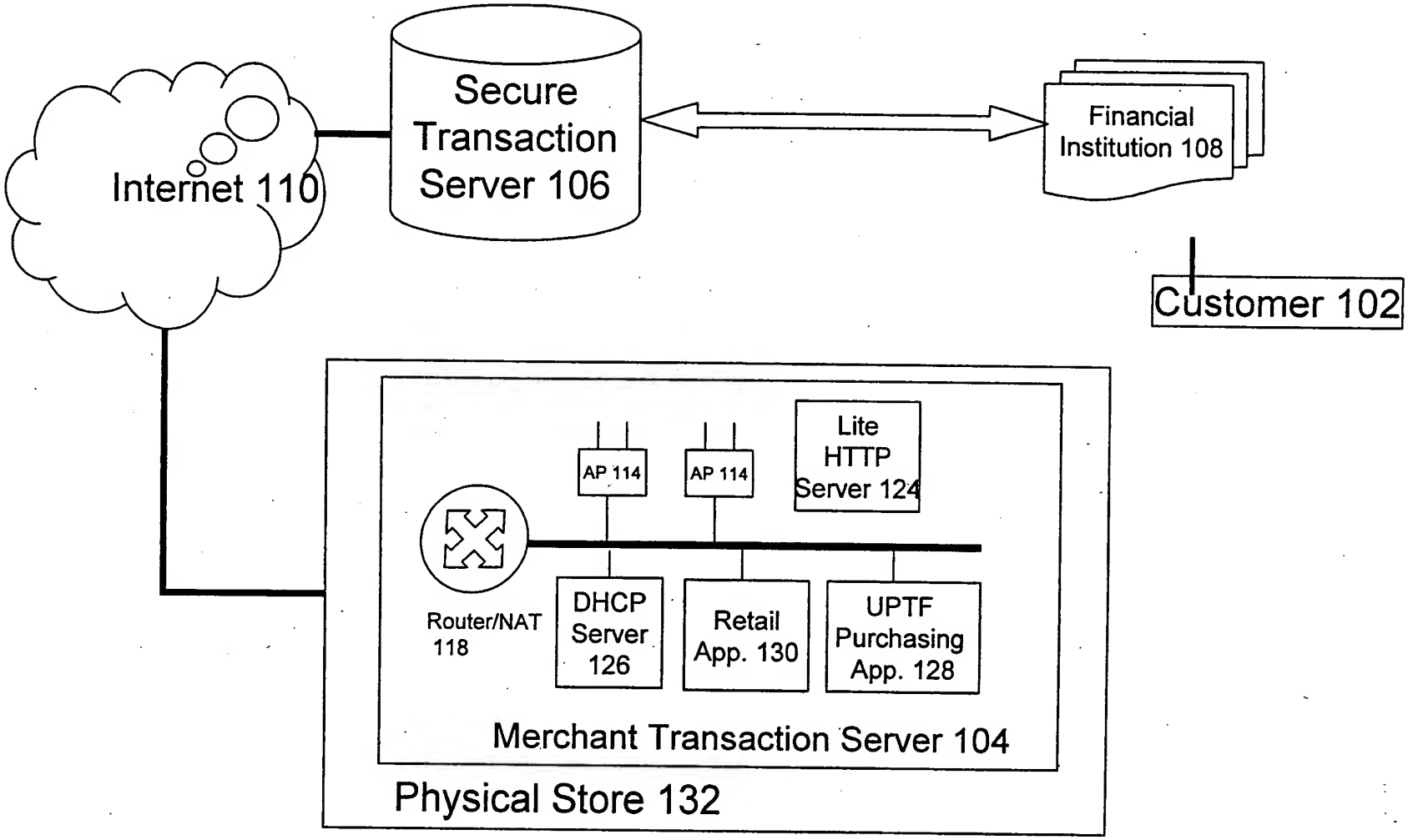

Internet 110
Secure Transaction Server 106
Financial Institution 108
Customer 102
AP 114
AP 114
Lite HTTP Server 124
Router/NAT 118
DHCP Server 126
Retail App. 130
UPTF Purchasing App. 128
Merchant Transaction Server 104
Physical Store 132

Figure 2

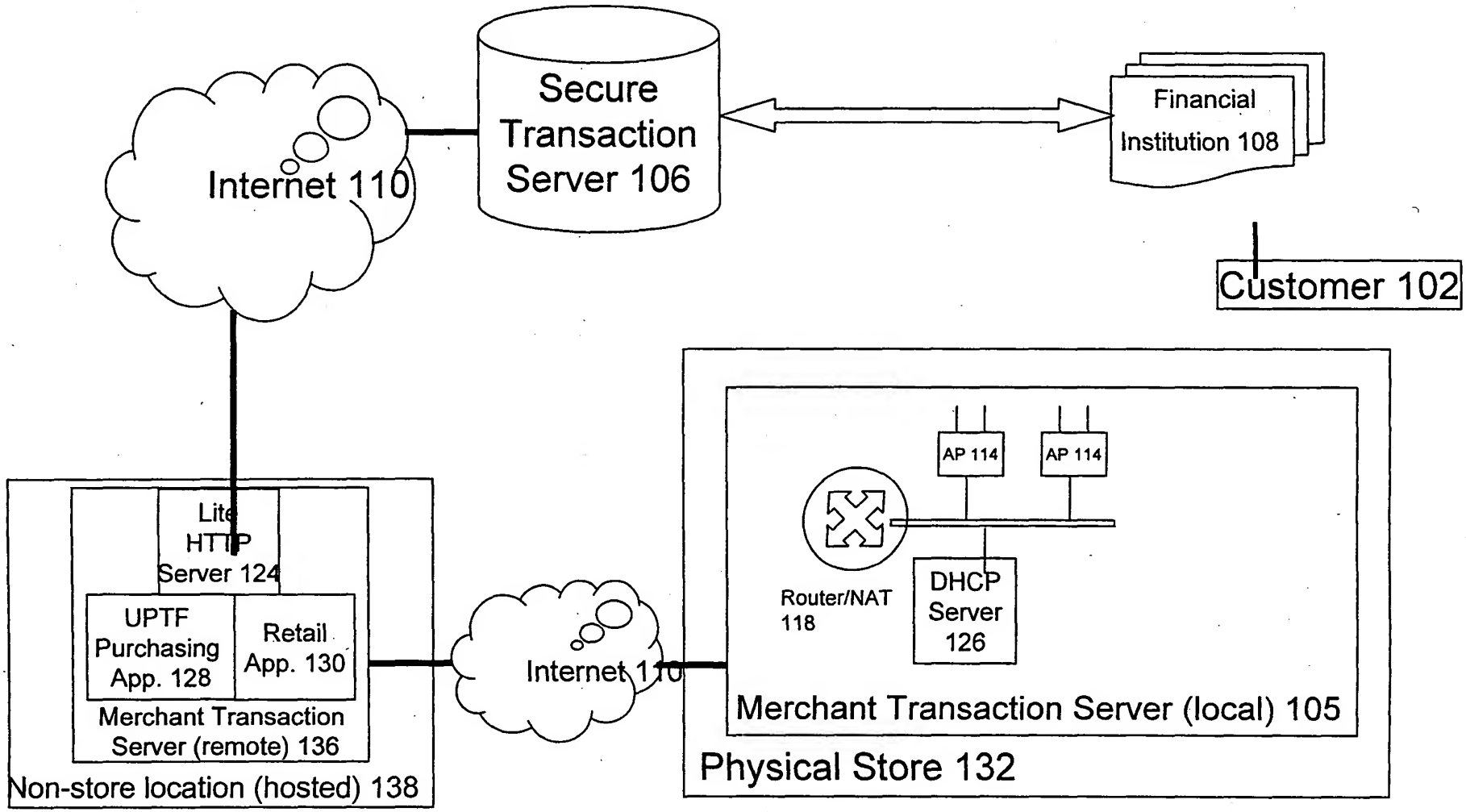

Secure
Transaction
Server 106
Internet 110
Financial
Institution 108
Customer 102
Lite
HTTP
Server 124
UPTF
Purchasing
App. 128
Retail
App. 130
Merchant Transaction
Server (remote) 136
Non-store location (hosted) 138
Internet 110
AP 114
AP 114
Router/NAT
118
DHCP
Server
126
Merchant Transaction Server (local) 105
Physical Store 132

Figure 3

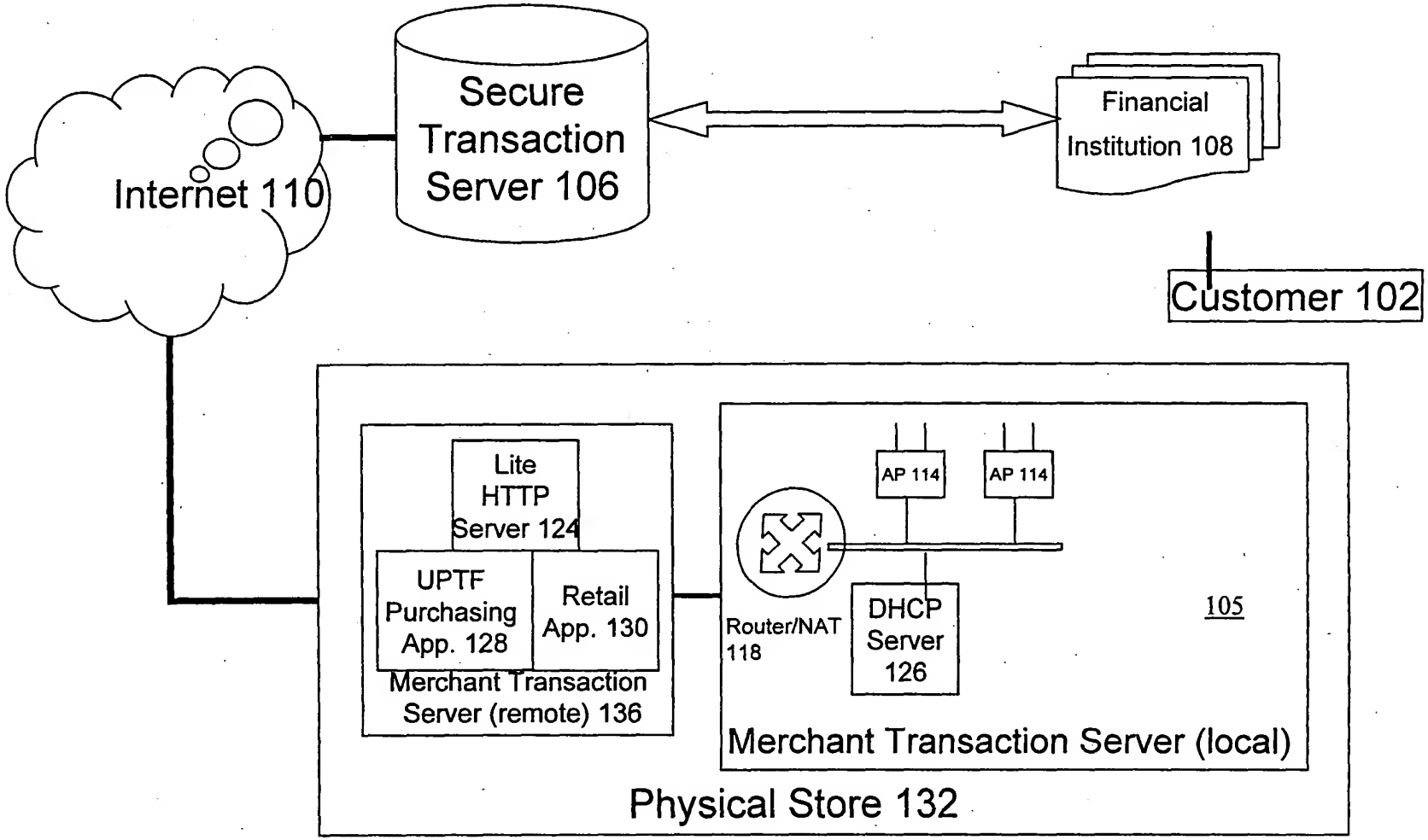

Internet 110
Secure Transaction Server 106
Financial Institution 108
Customer 102
Lite HTTP Server 124
UPTF Purchasing App. 128
Retail App. 130
Merchant Transaction Server (remote) 136
AP 114
AP 114
Router/NAT 118
DHCP Server 126
105
Merchant Transaction Server (local)
Physical Store 132

Figure 4

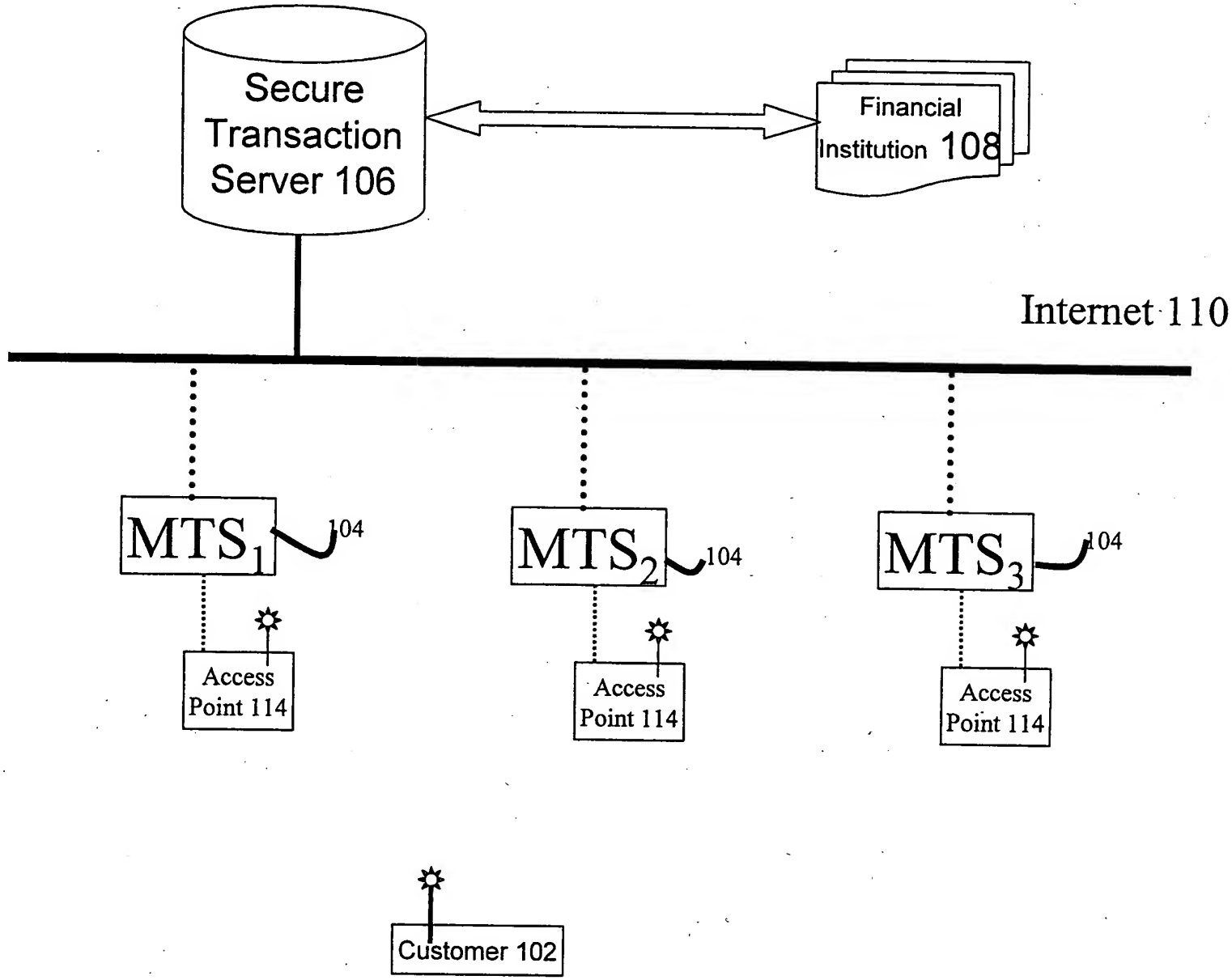

Secure Transaction Server 106
Financial Institution 108
Internet 110
MTS1
104
MTS2
104
MTS3
104
Access Point 114
Access Point 114
Access Point 114
Customer 102

Figure 5

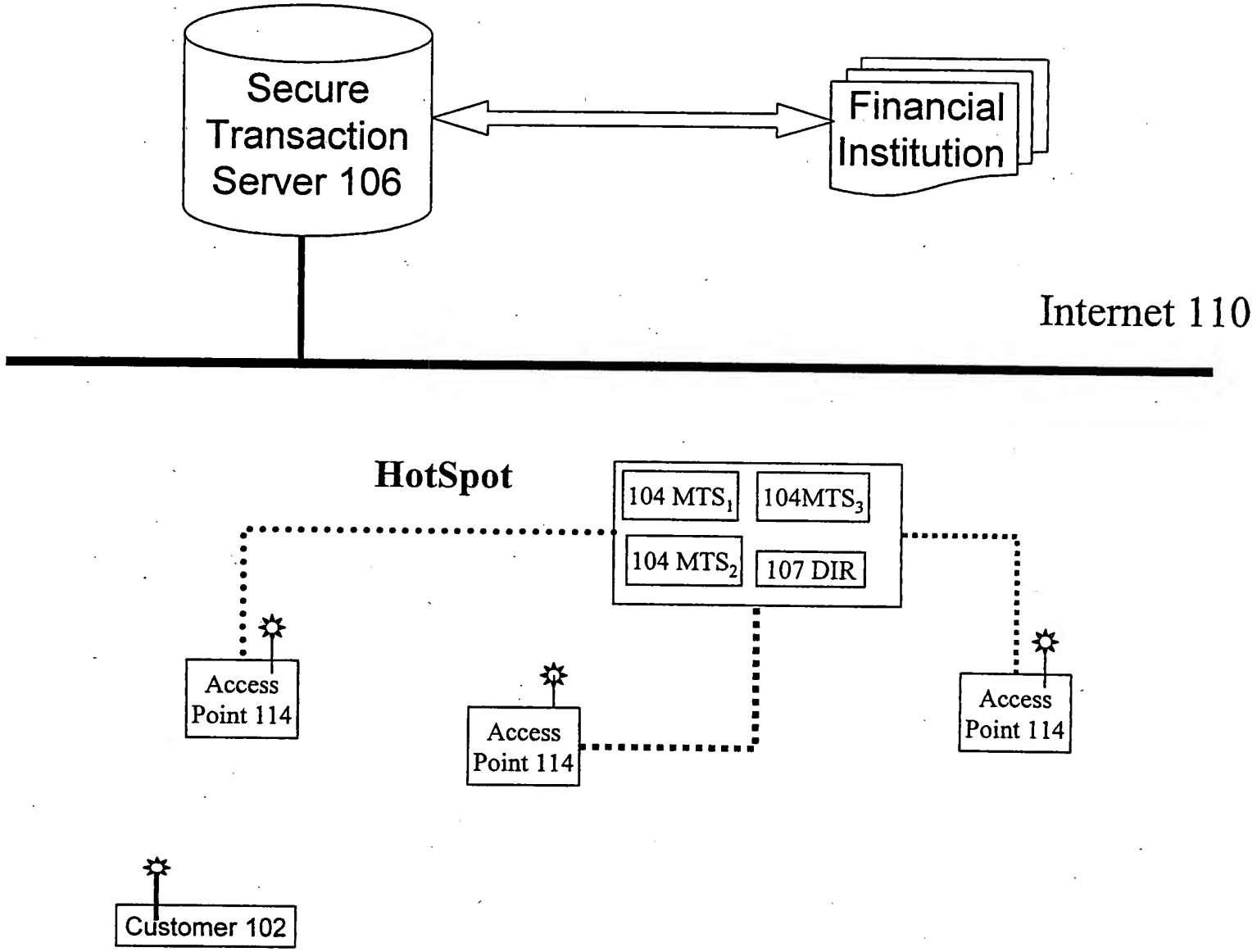

Secure
Transaction
Server 106
Financial
Institution
Internet 110
HotSpot
104 MTS1
104MTS3
104 MTS2
107 DIR
Access
Point 114
Access
Point 114
Access
Point 114
Customer 102

Figure 6

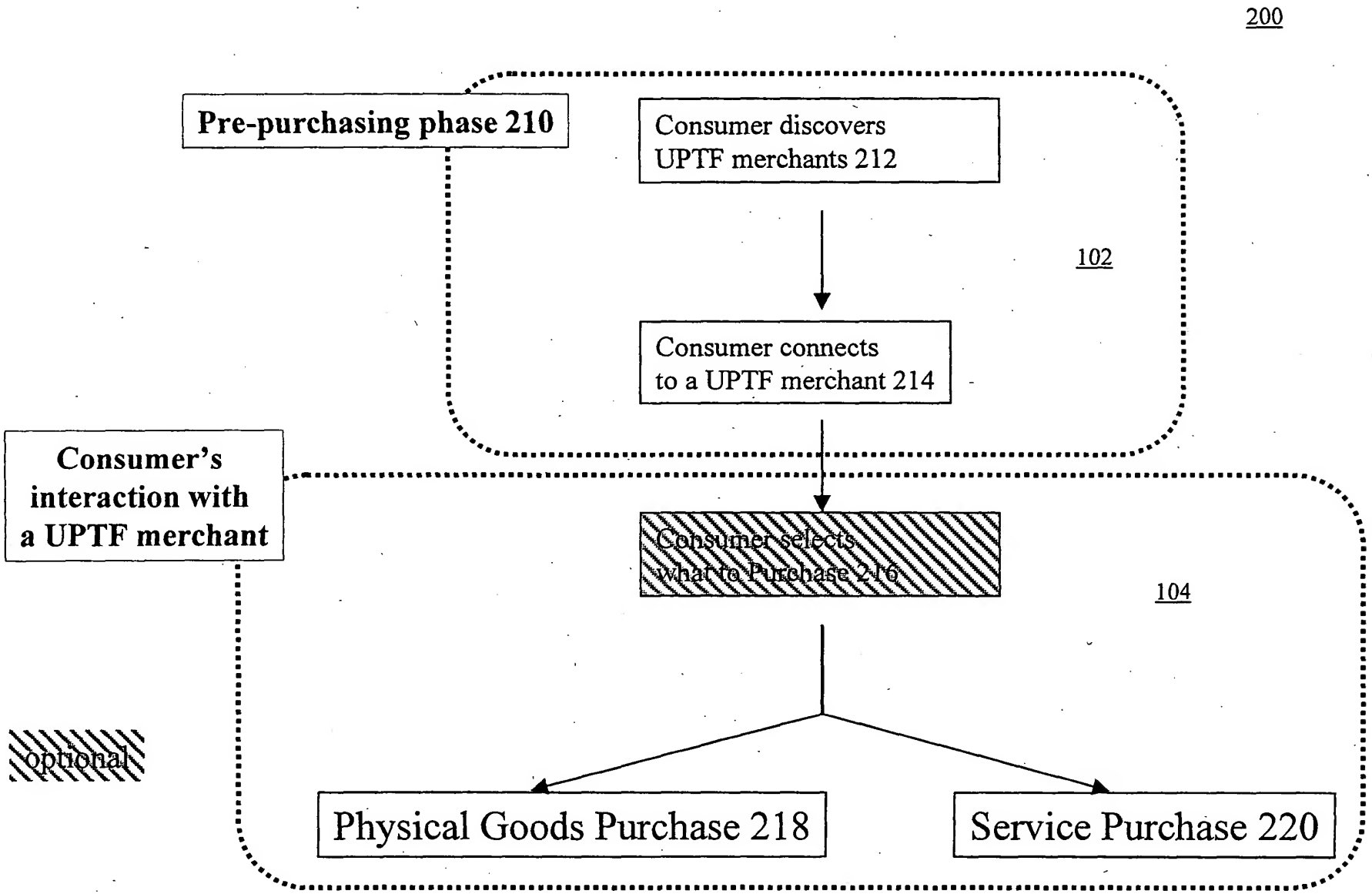

200
Pre-purchasing phase 210
Consumer discovers UPTF merchants 212
102
Consumer connects to a UPTF merchant 214
Consumer's interaction with a UPTF merchant
Consumer selects what to Purchase 216
104
optional
Physical Goods Purchase 218
Service Purchase 220

Figure 7

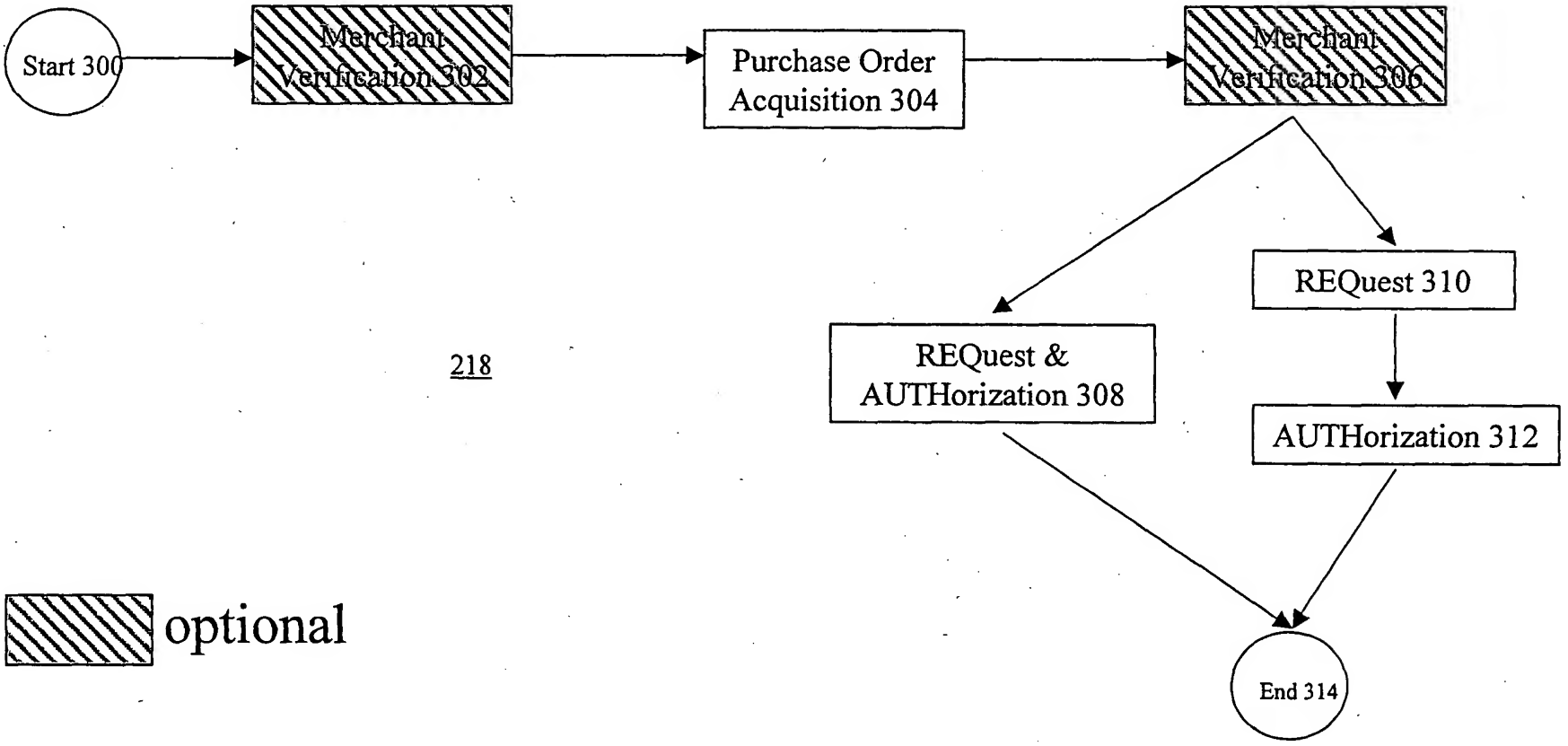

Start 300
Merchant Verification 302
Purchase Order Acquisition 304
Merchant Verification 306
REQuest 310
REQuest & AUTHorization 308
AUTHorization 312
End 314
218
optional

Figure 8

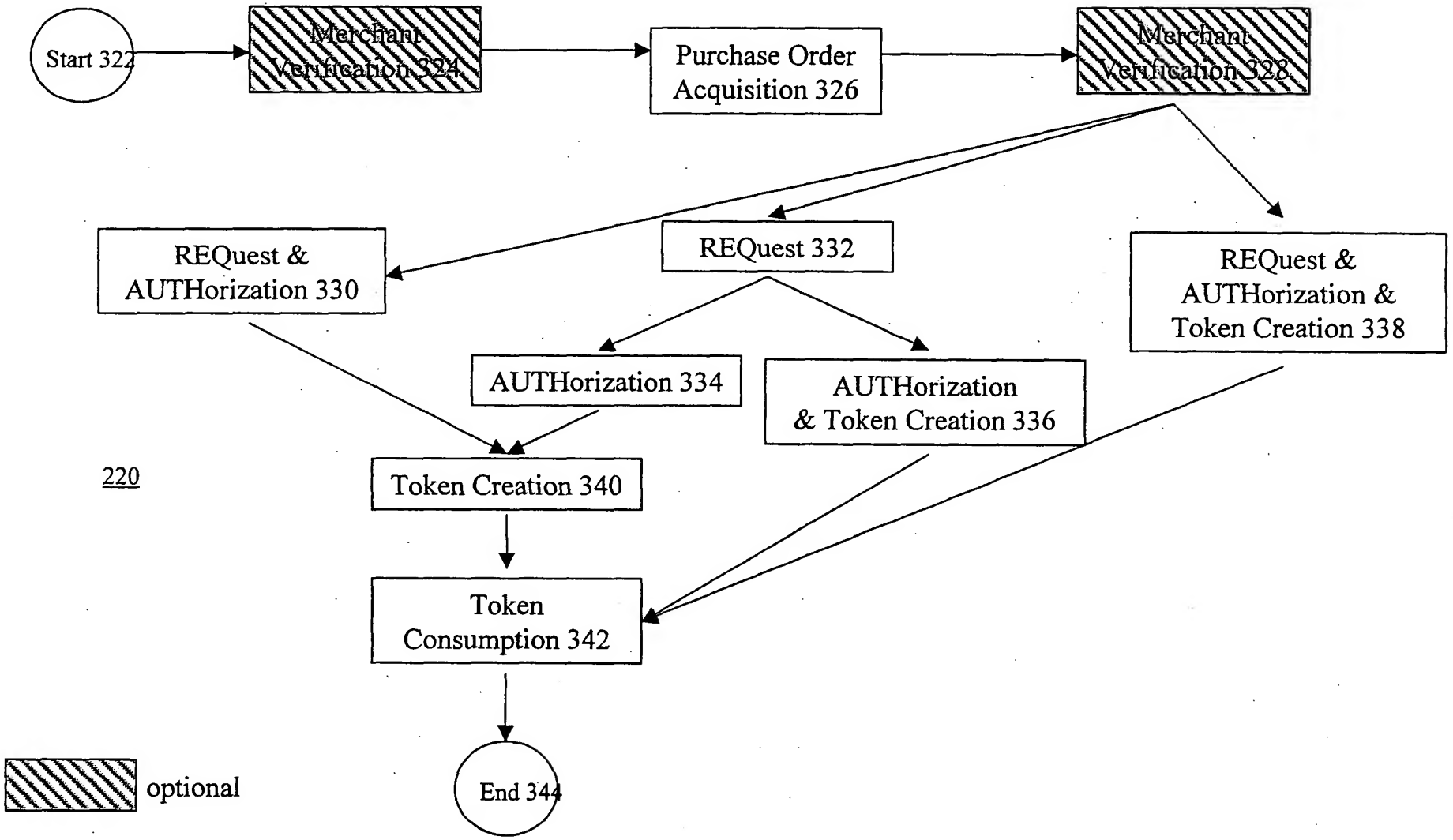

Start 322
Merchant Verification 324
Purchase Order Acquisition 326
Merchant Verification 328
REQuest & AUTHorization 330
REQuest 332
REQuest & AUTHorization & Token Creation 338
AUTHorization 334
AUTHorization & Token Creation 336
220
Token Creation 340
Token Consumption 342
End 344
optional

Figure 9

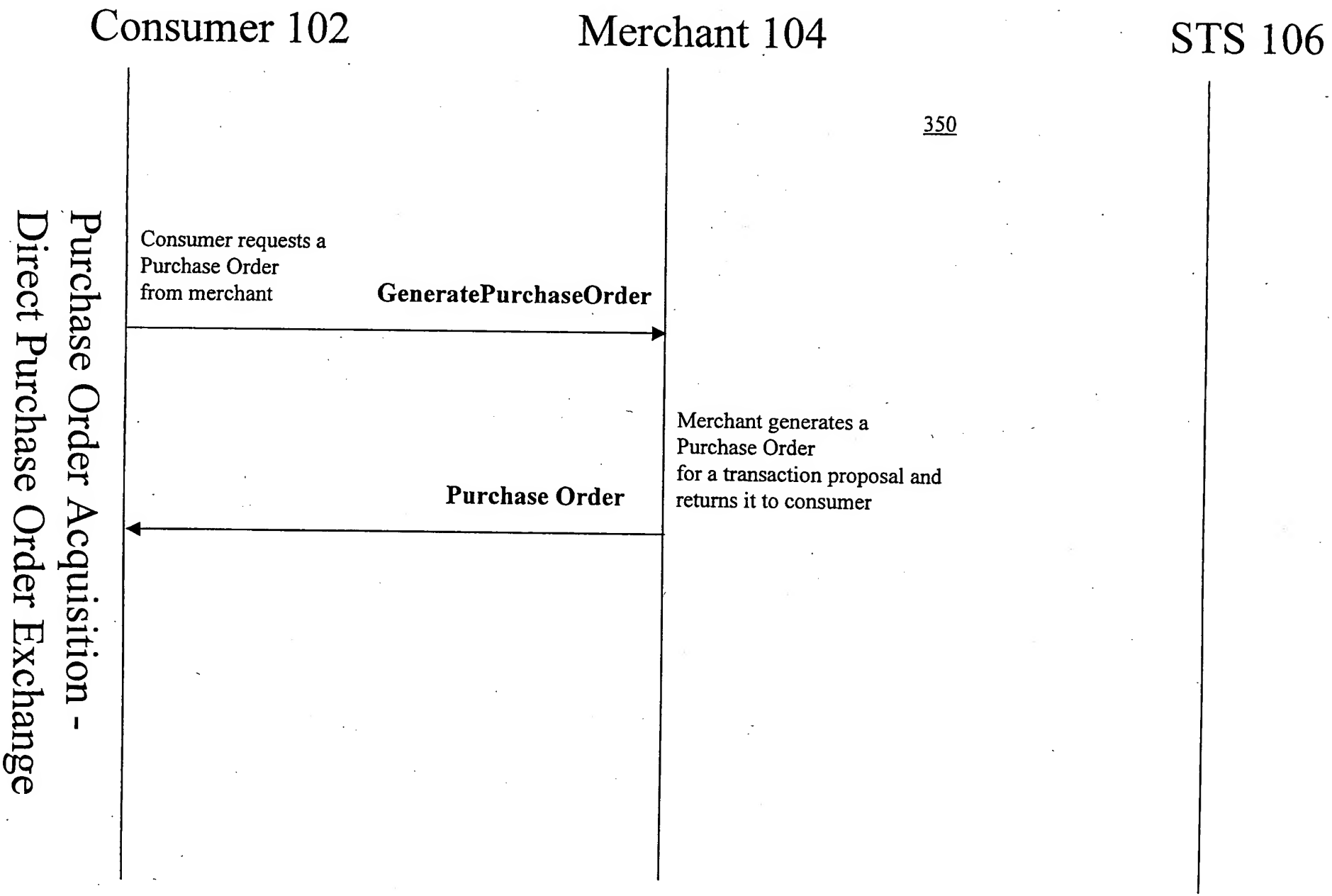

Consumer 102
Merchant 104
STS 106
350
Purchase Order Acquisition -
Direct Purchase Order Exchange
Consumer requests a
Purchase Order
from merchant
GeneratePurchaseOrder
Merchant generates a
Purchase Order
for a transaction proposal and
returns it to consumer
Purchase Order

Figure 10

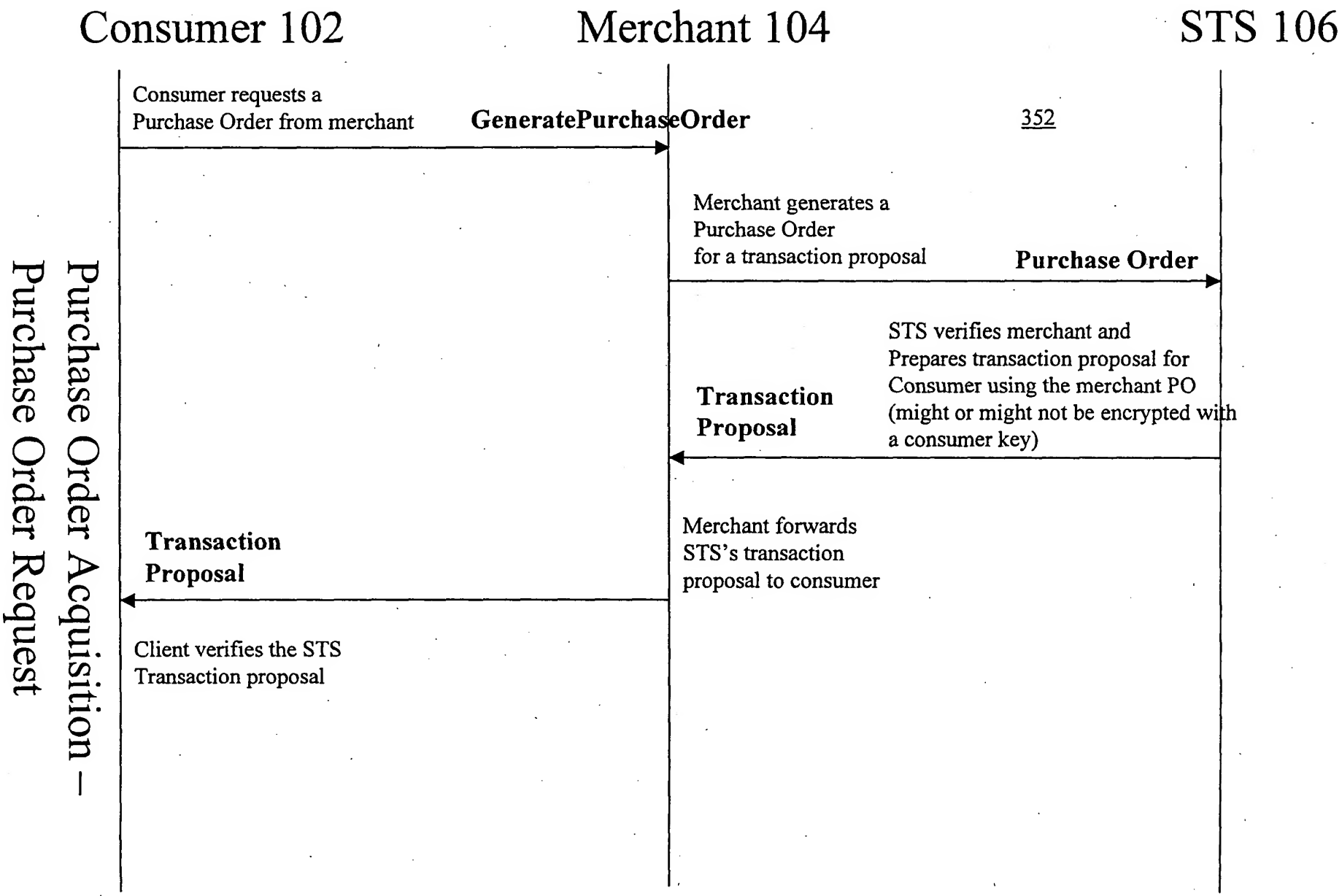

Consumer 102
Merchant 104
STS 106
Purchase Order Acquisition – Purchase Order Request
Consumer requests a Purchase Order from merchant
GeneratePurchaseOrder
352
Merchant generates a Purchase Order for a transaction proposal
Purchase Order
STS verifies merchant and Prepares transaction proposal for Consumer using the merchant PO (might or might not be encrypted with a consumer key)
Transaction Proposal
Merchant forwards STS's transaction proposal to consumer
Transaction Proposal
Client verifies the STS Transaction proposal

Figure 11

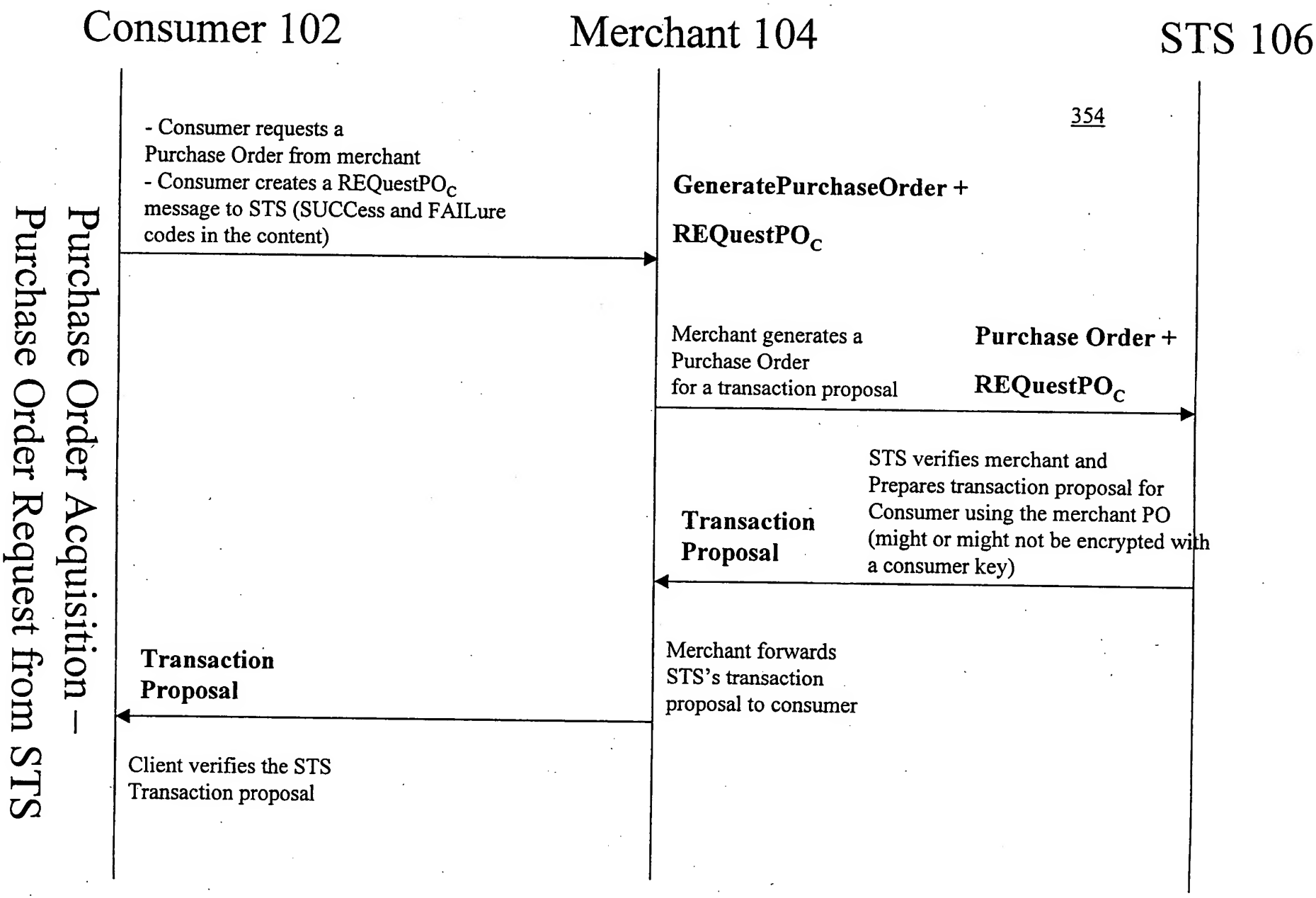

Consumer 102
Merchant 104
STS 106
Purchase Order Acquisition – Purchase Order Request from STS
354
- Consumer requests a Purchase Order from merchant
- Consumer creates a REQuestPO$_C$ message to STS (SUCCess and FAILure codes in the content)
GeneratePurchaseOrder + REQuestPO$_C$
Merchant generates a Purchase Order for a transaction proposal
Purchase Order + REQuestPO$_C$
STS verifies merchant and Prepares transaction proposal for Consumer using the merchant PO (might or might not be encrypted with a consumer key)
Transaction Proposal
Merchant forwards STS's transaction proposal to consumer
Transaction Proposal
Client verifies the STS Transaction proposal

Figure 12

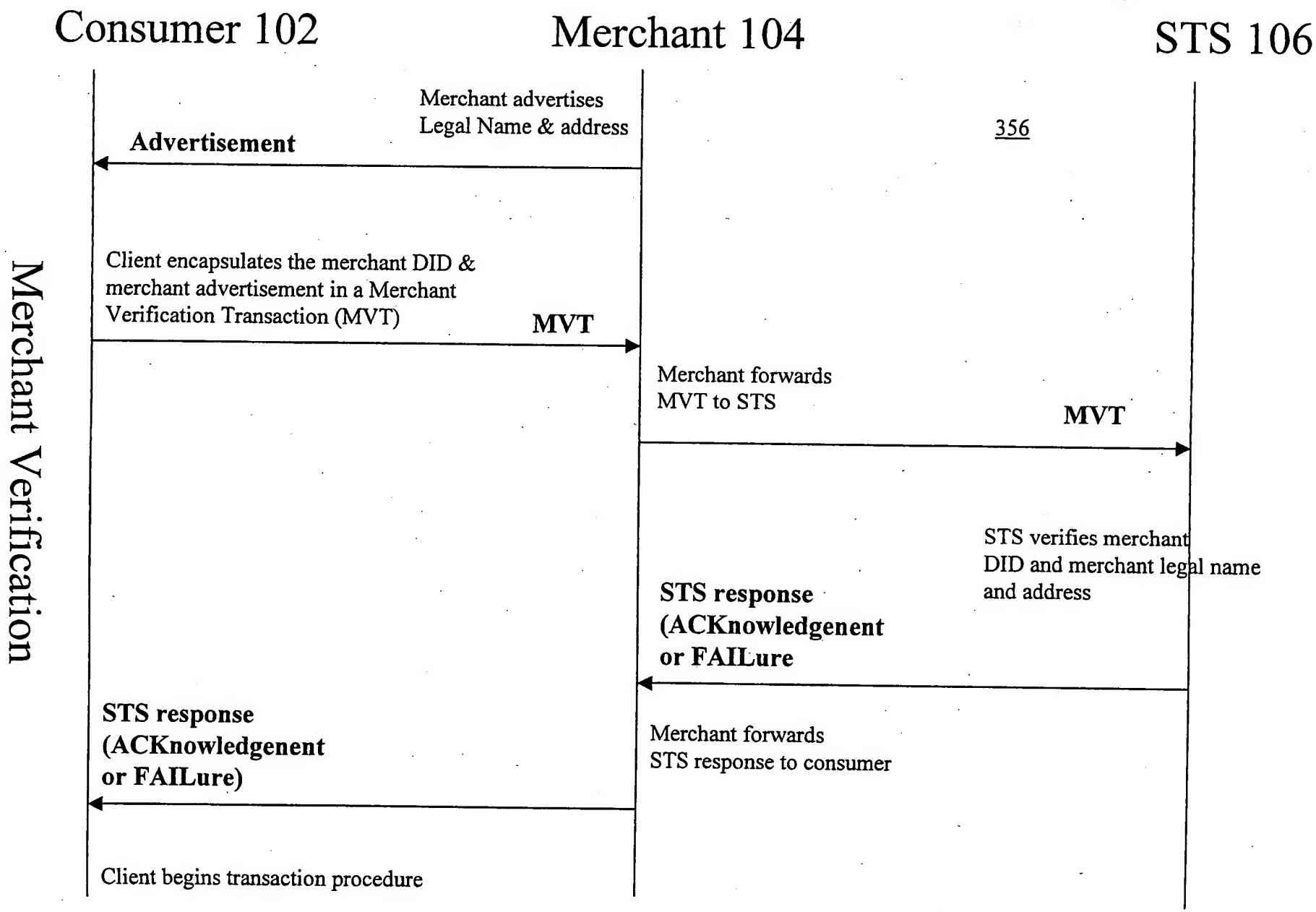

Consumer 102
Merchant 104
STS 106
Merchant Verification
Merchant advertises
Legal Name & address
356
Advertisement
Client encapsulates the merchant DID &
merchant advertisement in a Merchant
Verification Transaction (MVT)
MVT
Merchant forwards
MVT to STS
MVT
STS verifies merchant
DID and merchant legal name
and address
STS response
(ACKnowledgenent
or FAILure
STS response
(ACKnowledgenent
or FAILure)
Merchant forwards
STS response to consumer
Client begins transaction procedure

Figure 13

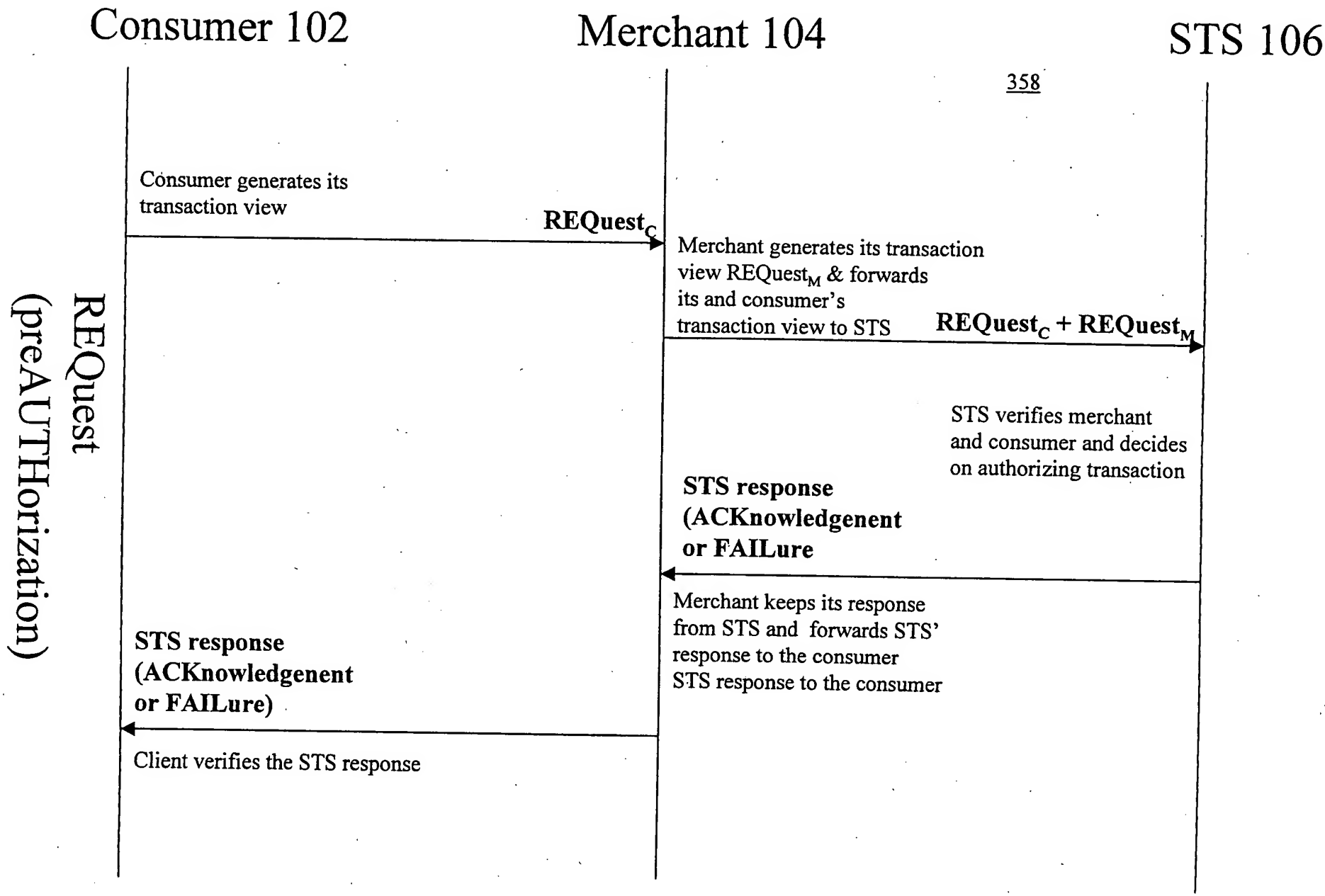

Consumer 102
Merchant 104
STS 106
358
REQuest (preAUTHorization)
Consumer generates its transaction view
REQuest$_C$
Merchant generates its transaction view REQuest$_M$ & forwards its and consumer's transaction view to STS
REQuest$_C$ + REQuest$_M$
STS verifies merchant and consumer and decides on authorizing transaction
STS response (ACKnowledgenent or FAILure
Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consumer
STS response (ACKnowledgenent or FAILure)
Client verifies the STS response

Figure 14

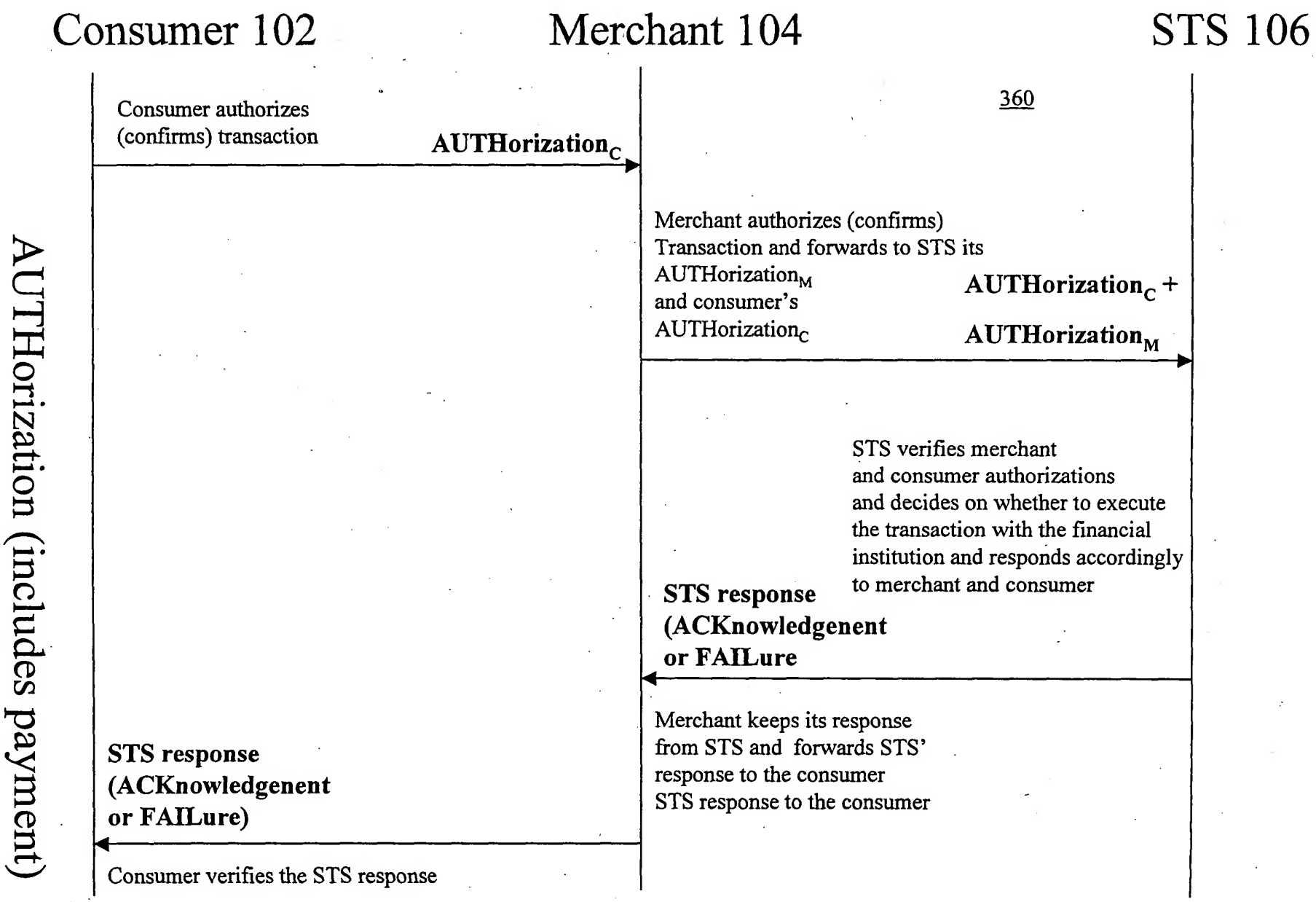

Consumer 102
Merchant 104
STS 106
AUTHorization (includes payment)
Consumer authorizes (confirms) transaction
AUTHorization$_C$
360
Merchant authorizes (confirms) Transaction and forwards to STS its AUTHorization$_M$ and consumer's AUTHorization$_C$
AUTHorization$_C$ + AUTHorization$_M$
STS verifies merchant and consumer authorizations and decides on whether to execute the transaction with the financial institution and responds accordingly to merchant and consumer
STS response (ACKnowledgenent or FAILure
Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consumer
STS response (ACKnowledgenent or FAILure)
Consumer verifies the STS response

Figure 15

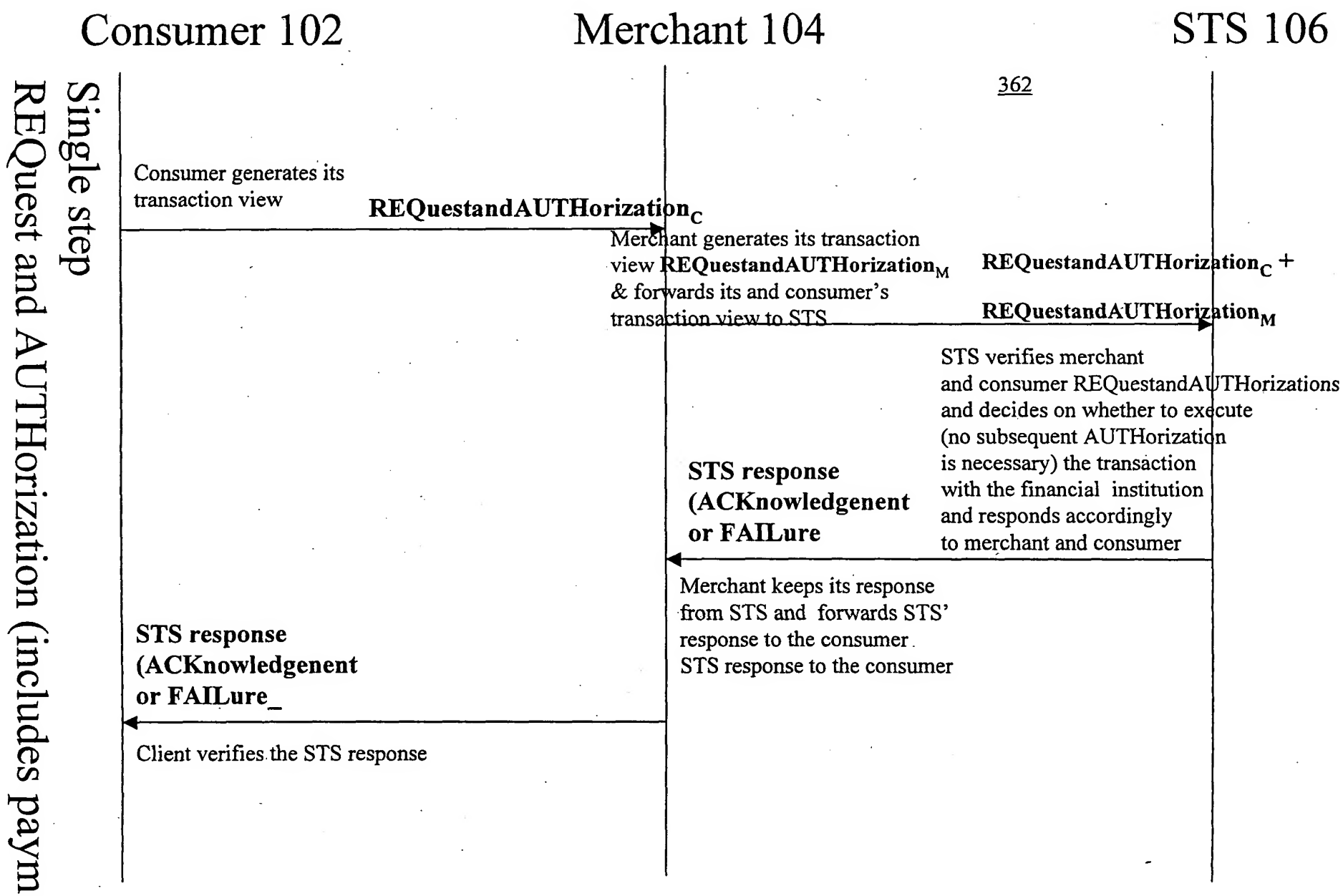

Consumer 102
Merchant 104
STS 106
Single step
REQuest and AUTHorization (includes payment)
362
Consumer generates its transaction view
REQuestandAUTHorization$_C$
Merchant generates its transaction view REQuestandAUTHorization$_M$ & forwards its and consumer's transaction view to STS
REQuestandAUTHorization$_C$ +
REQuestandAUTHorization$_M$
STS verifies merchant and consumer REQuestandAUTHorizations and decides on whether to execute (no subsequent AUTHorization is necessary) the transaction with the financial institution and responds accordingly to merchant and consumer
STS response (ACKnowledgenent or FAILure
Merchant keeps its response from STS and forwards STS' response to the consumer.
STS response to the consumer
STS response (ACKnowledgenent or FAILure_
Client verifies the STS response

Figure 16

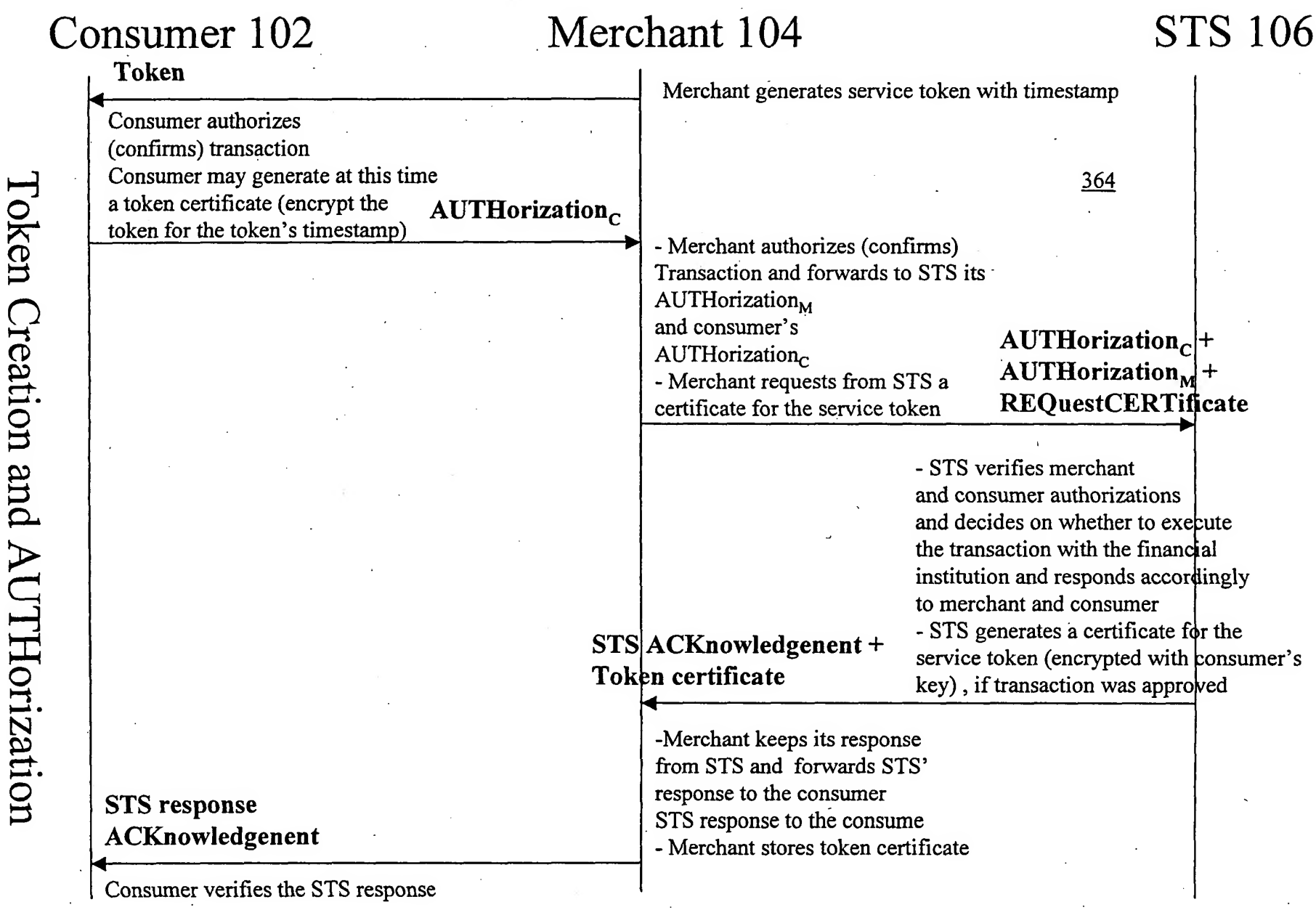

Consumer 102
Merchant 104
STS 106
Token Creation and AUTHorization
Token
Merchant generates service token with timestamp
Consumer authorizes (confirms) transaction
Consumer may generate at this time a token certificate (encrypt the token for the token's timestamp)
AUTHorization$_C$
364
- Merchant authorizes (confirms) Transaction and forwards to STS its AUTHorization$_M$ and consumer's AUTHorization$_C$
- Merchant requests from STS a certificate for the service token
AUTHorization$_C$ + AUTHorization$_M$ + REQuestCERTificate
- STS verifies merchant and consumer authorizations and decides on whether to execute the transaction with the financial institution and responds accordingly to merchant and consumer
- STS generates a certificate for the service token (encrypted with consumer's key) , if transaction was approved
STS ACKnowledgenent + Token certificate
-Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consume
- Merchant stores token certificate
STS response ACKnowledgenent
Consumer verifies the STS response

Figure 17

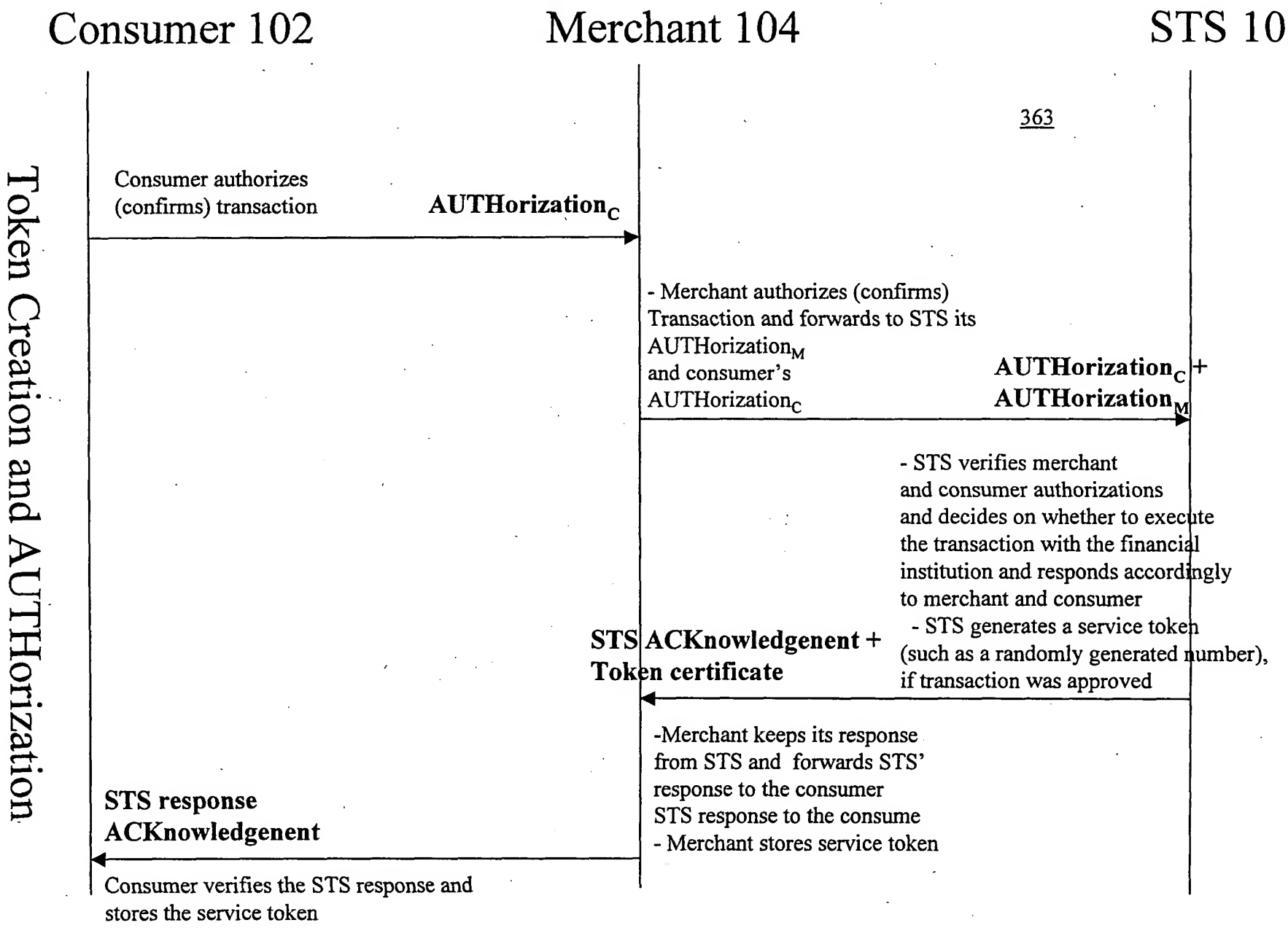

Consumer 102
Merchant 104
STS 106
Token Creation and AUTHorization
363
Consumer authorizes (confirms) transaction
AUTHorization$_C$
- Merchant authorizes (confirms) Transaction and forwards to STS its AUTHorization$_M$ and consumer's AUTHorization$_C$
AUTHorization$_C$ + AUTHorization$_M$
- STS verifies merchant and consumer authorizations and decides on whether to execute the transaction with the financial institution and responds accordingly to merchant and consumer
- STS generates a service token (such as a randomly generated number), if transaction was approved
STS ACKnowledgenent + Token certificate
-Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consume
- Merchant stores service token
STS response ACKnowledgenent
Consumer verifies the STS response and stores the service token

Figure 18

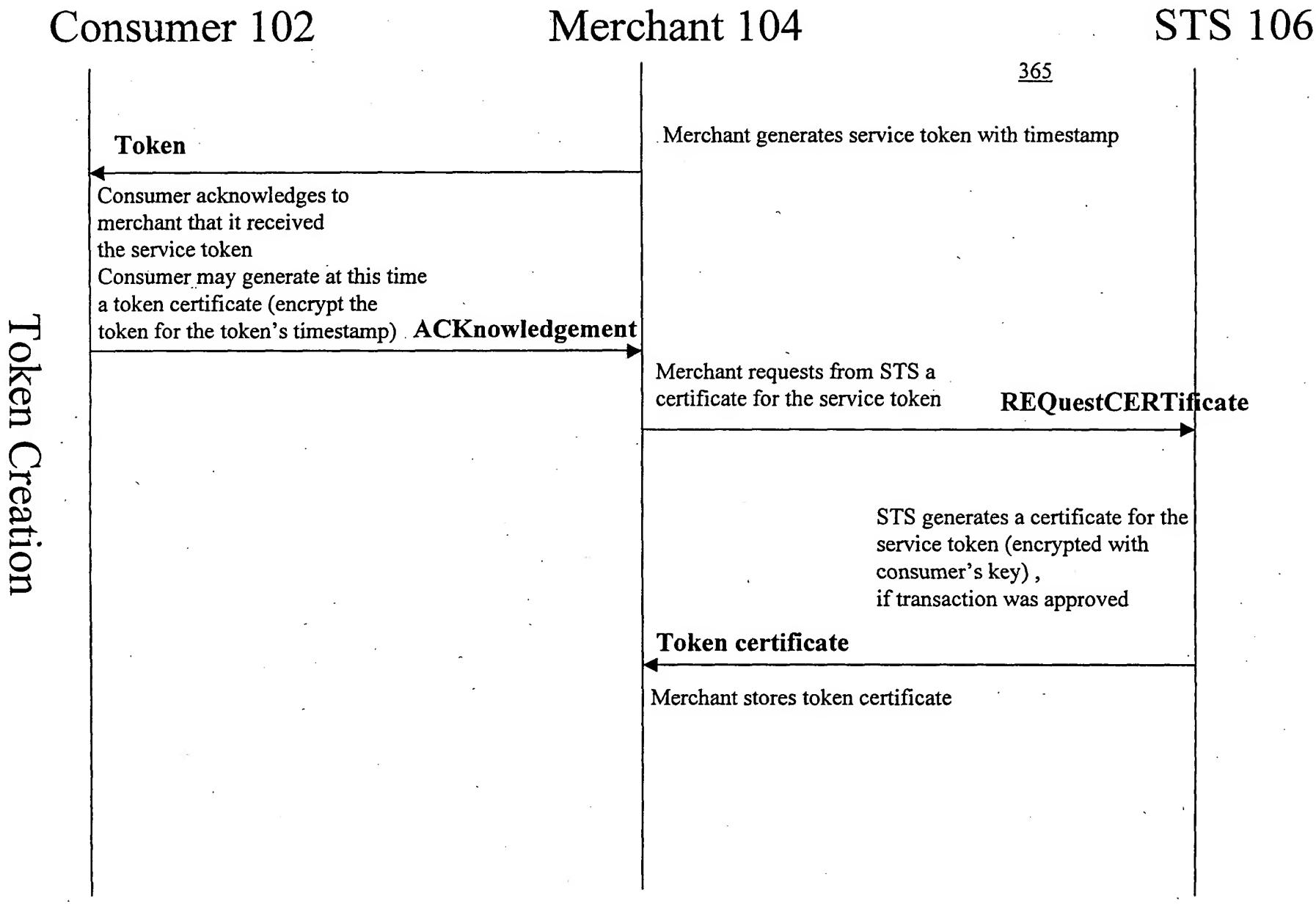

Consumer 102
Merchant 104
STS 106
Token Creation
365
Merchant generates service token with timestamp
Token
Consumer acknowledges to merchant that it received the service token
Consumer may generate at this time a token certificate (encrypt the token for the token's timestamp)
ACKnowledgement
Merchant requests from STS a certificate for the service token
REQuestCERTificate
STS generates a certificate for the service token (encrypted with consumer's key) , if transaction was approved
Token certificate
Merchant stores token certificate

Figure 19

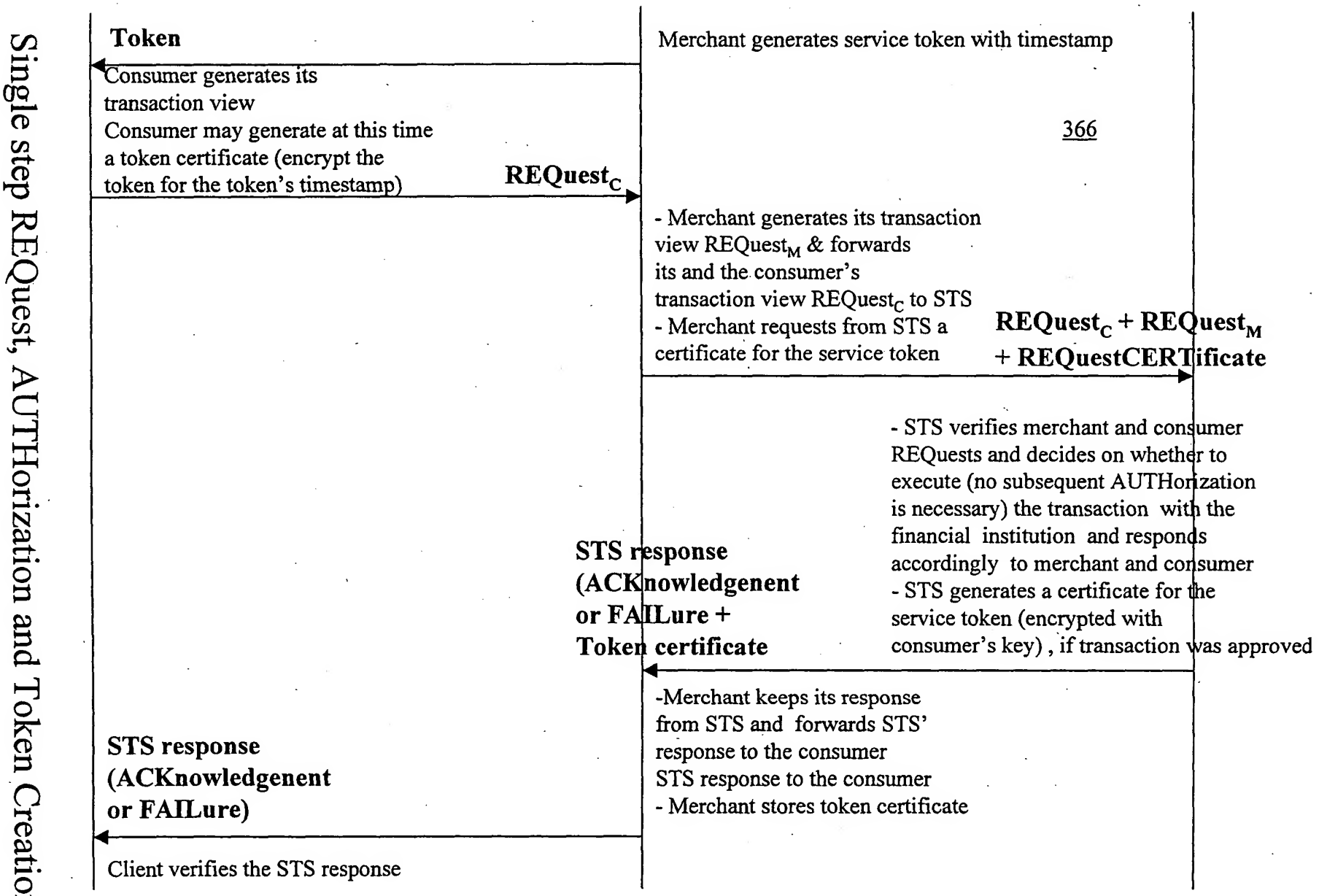

Consumer 102
Merchant 104
STS 106
Single step REQuest, AUTHorization and Token Creation
Token
Merchant generates service token with timestamp
Consumer generates its transaction view
Consumer may generate at this time a token certificate (encrypt the token for the token's timestamp)
366
REQuest$_C$
- Merchant generates its transaction view REQuest$_M$ & forwards its and the consumer's transaction view REQuest$_C$ to STS
- Merchant requests from STS a certificate for the service token
REQuest$_C$ + REQuest$_M$ + REQuestCERTificate
- STS verifies merchant and consumer REQuests and decides on whether to execute (no subsequent AUTHorization is necessary) the transaction with the financial institution and responds accordingly to merchant and consumer
- STS generates a certificate for the service token (encrypted with consumer's key) , if transaction was approved
STS response (ACKnowledgenent or FAILure + Token certificate
-Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consumer
- Merchant stores token certificate
STS response (ACKnowledgenent or FAILure)
Client verifies the STS response

Figure 20

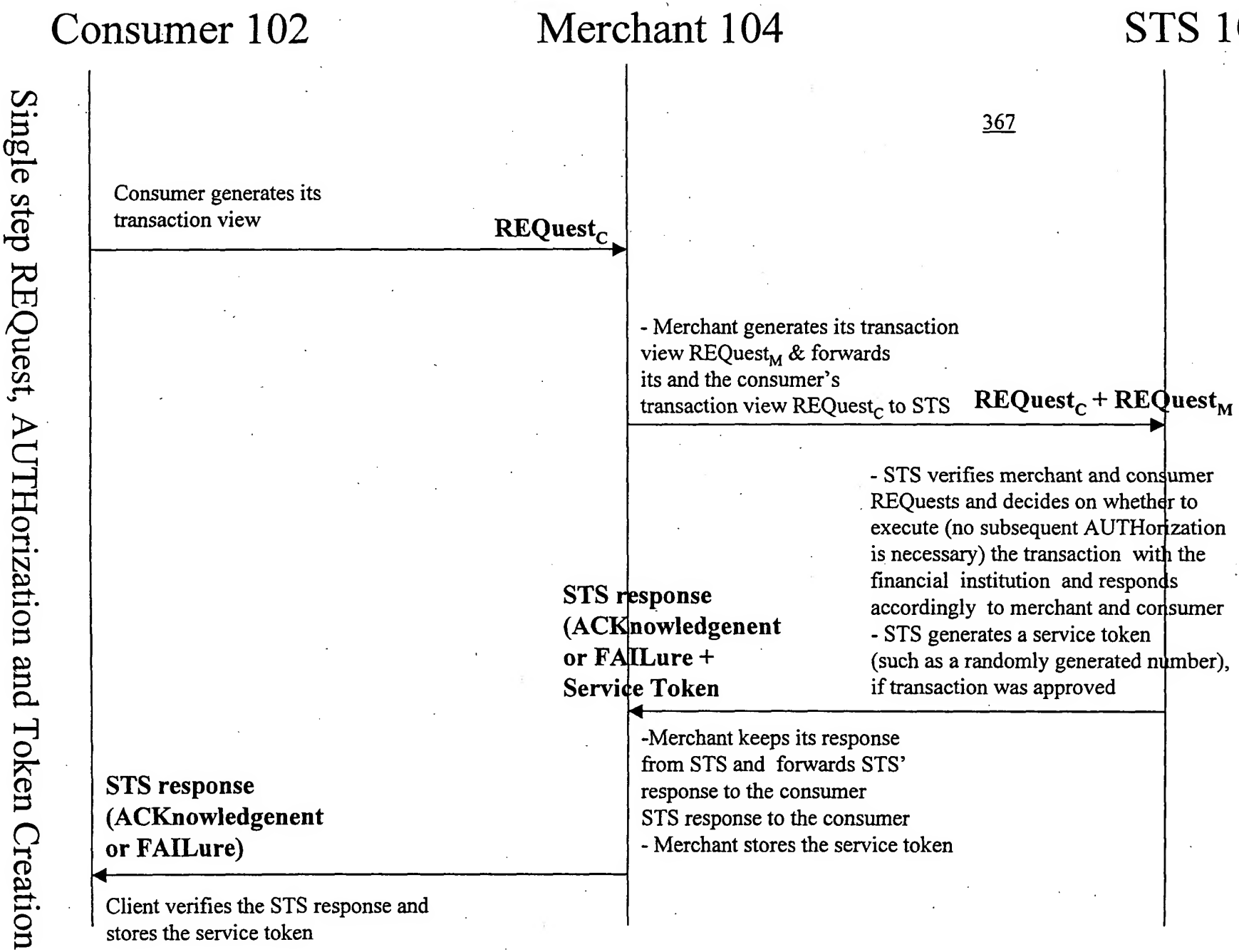

Consumer 102
Merchant 104
STS 106
Single step REQuest, AUTHorization and Token Creation
367
Consumer generates its transaction view
REQuest$_C$
- Merchant generates its transaction view REQuest$_M$ & forwards its and the consumer's transaction view REQuest$_C$ to STS
REQuest$_C$ + REQuest$_M$
- STS verifies merchant and consumer REQuests and decides on whether to execute (no subsequent AUTHorization is necessary) the transaction with the financial institution and responds accordingly to merchant and consumer
- STS generates a service token (such as a randomly generated number), if transaction was approved
STS response (ACKnowledgenent or FAILure + Service Token
-Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consumer
- Merchant stores the service token
STS response (ACKnowledgenent or FAILure)
Client verifies the STS response and stores the service token

Figure 21

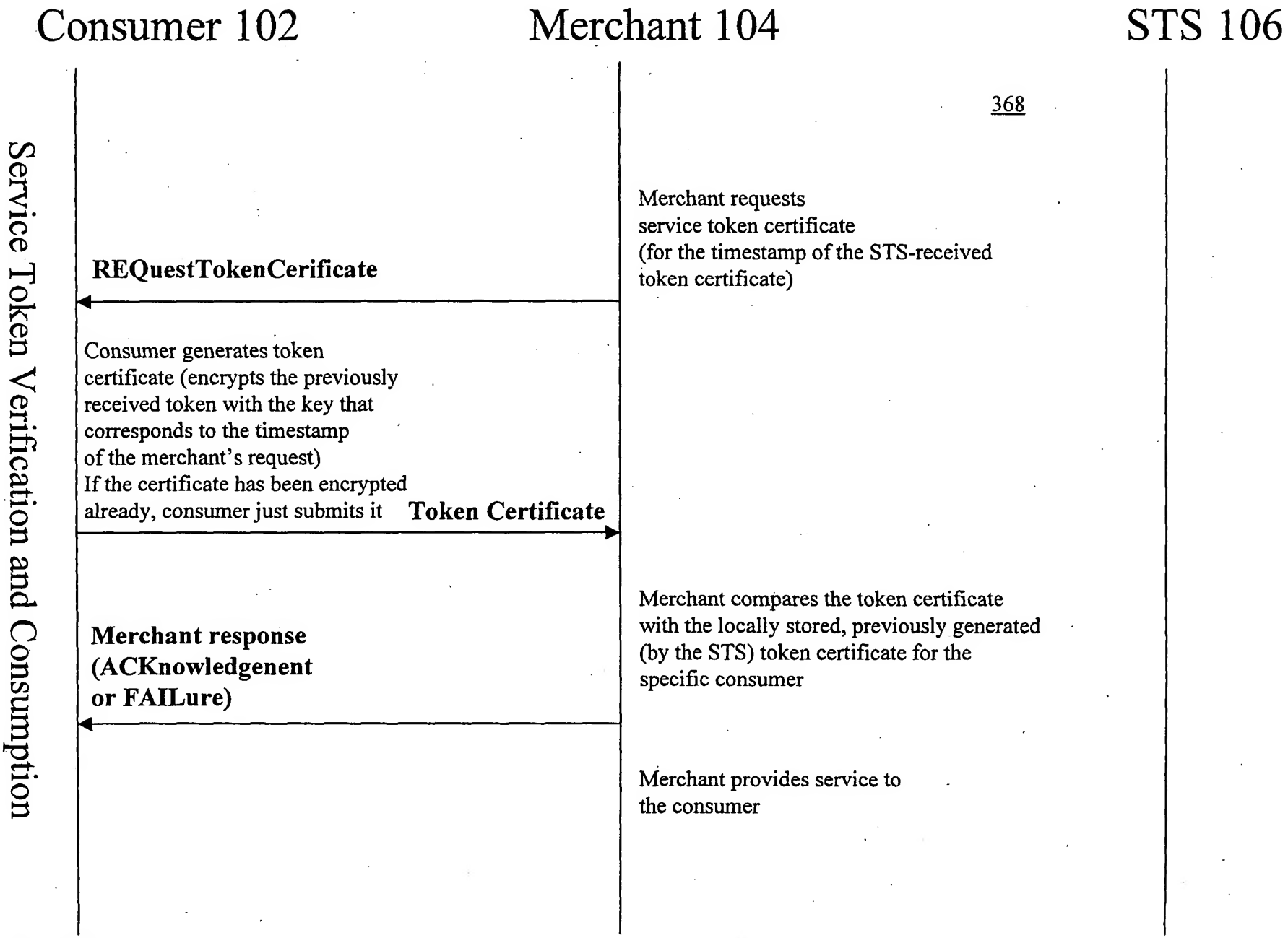

Consumer 102
Merchant 104
STS 106
Service Token Verification and Consumption
368
Merchant requests
service token certificate
(for the timestamp of the STS-received
token certificate)
REQuestTokenCerificate
Consumer generates token
certificate (encrypts the previously
received token with the key that
corresponds to the timestamp
of the merchant's request)
If the certificate has been encrypted
already, consumer just submits it
Token Certificate
Merchant compares the token certificate
with the locally stored, previously generated
(by the STS) token certificate for the
specific consumer
Merchant response
(ACKnowledgenent
or FAILure)
Merchant provides service to
the consumer

Figure 22

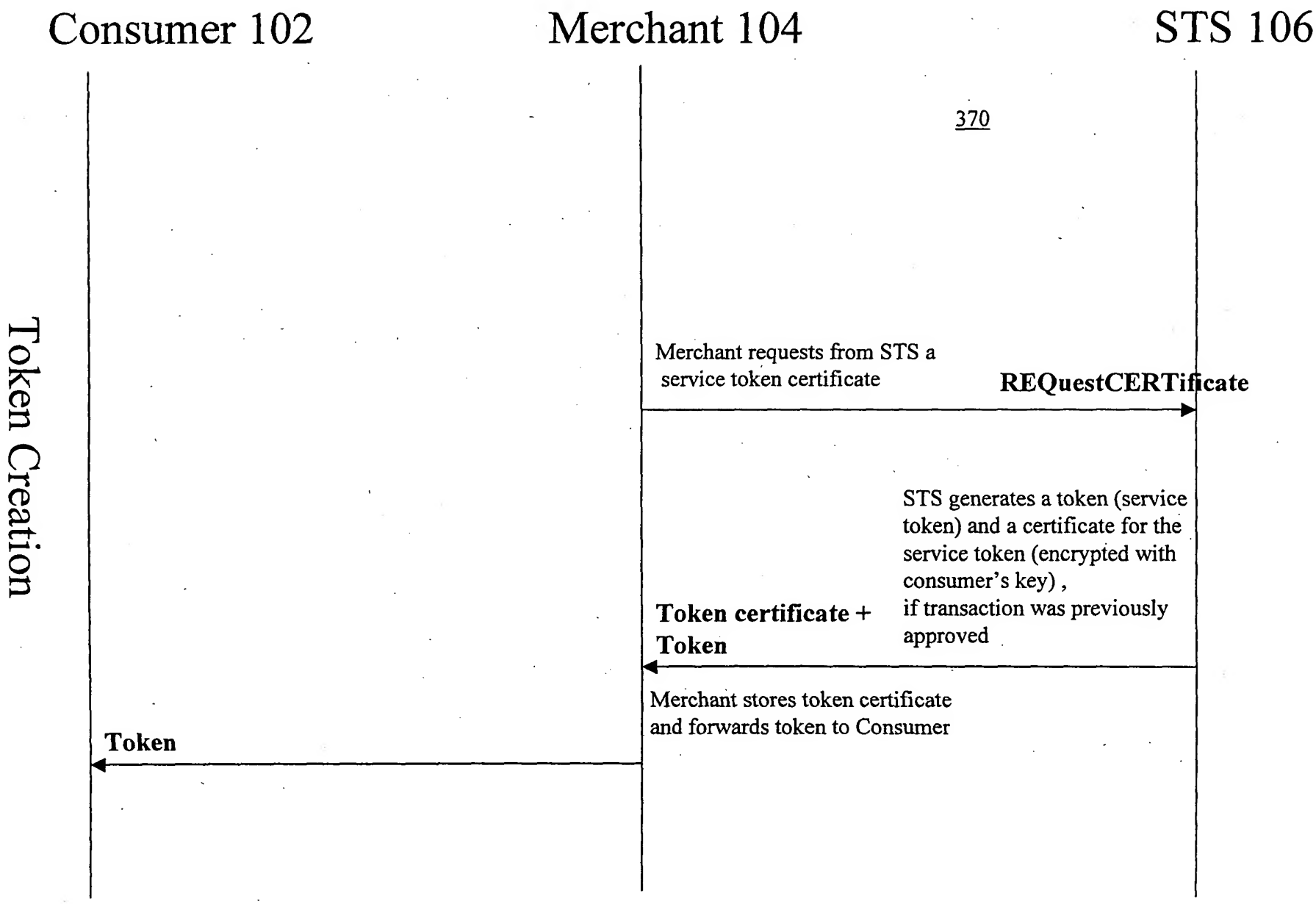

Consumer 102
Merchant 104
STS 106
370
Token Creation
Merchant requests from STS a service token certificate
REQuestCERTificate
STS generates a token (service token) and a certificate for the service token (encrypted with consumer's key) , if transaction was previously approved
Token certificate + Token
Merchant stores token certificate and forwards token to Consumer
Token

Figure 23

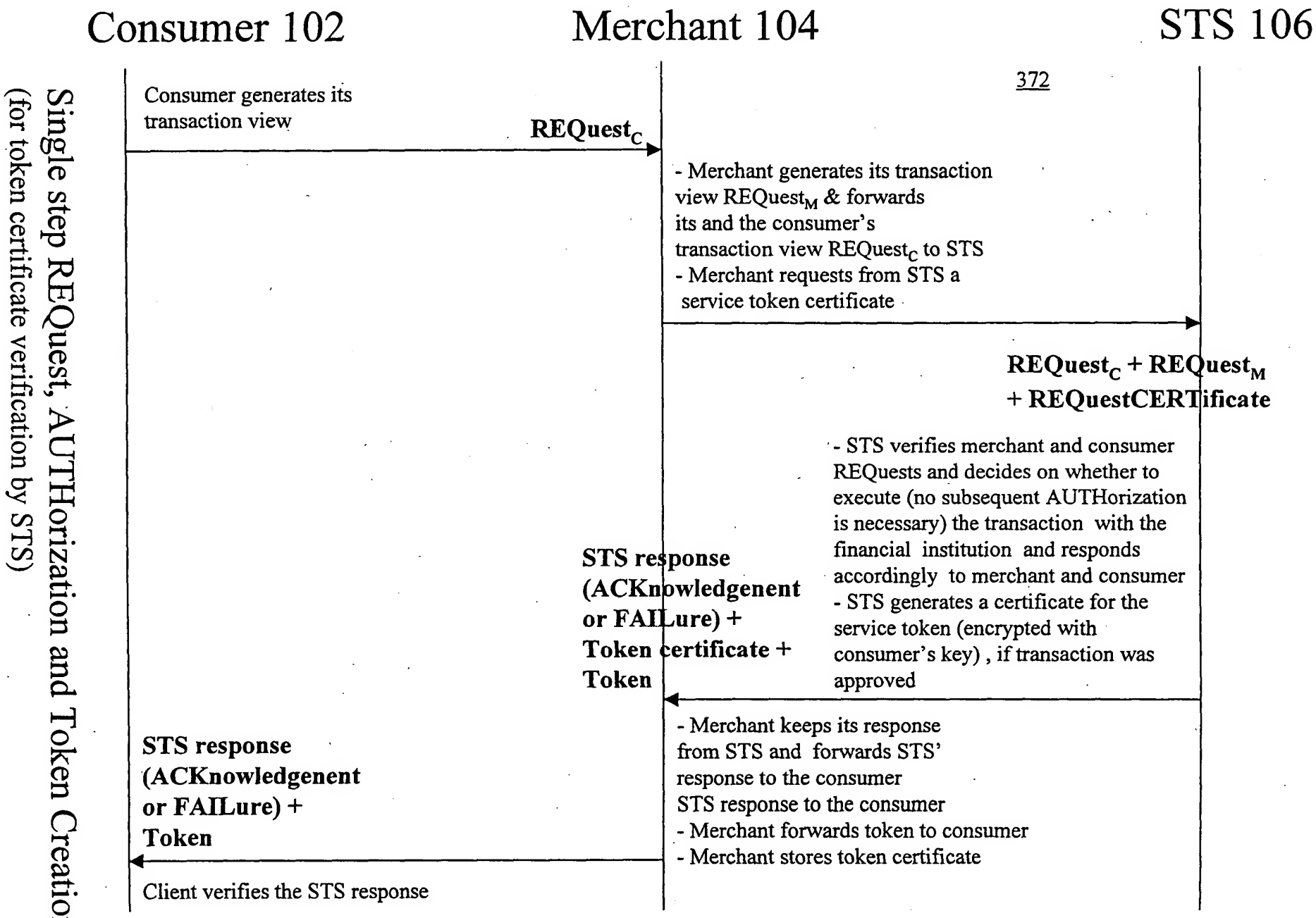

Consumer 102
Merchant 104
STS 106
Single step REQuest, AUTHorization and Token Creation
(for token certificate verification by STS)
372
Consumer generates its transaction view
REQuest$_C$
- Merchant generates its transaction view REQuest$_M$ & forwards its and the consumer's transaction view REQuest$_C$ to STS
- Merchant requests from STS a service token certificate
REQuest$_C$ + REQuest$_M$ + REQuestCERTificate
- STS verifies merchant and consumer REQuests and decides on whether to execute (no subsequent AUTHorization is necessary) the transaction with the financial institution and responds accordingly to merchant and consumer
- STS generates a certificate for the service token (encrypted with consumer's key) , if transaction was approved
STS response (ACKnowledgenent or FAILure) + Token certificate + Token
- Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consumer
- Merchant forwards token to consumer
- Merchant stores token certificate
STS response (ACKnowledgenent or FAILure) + Token
Client verifies the STS response

Figure 24

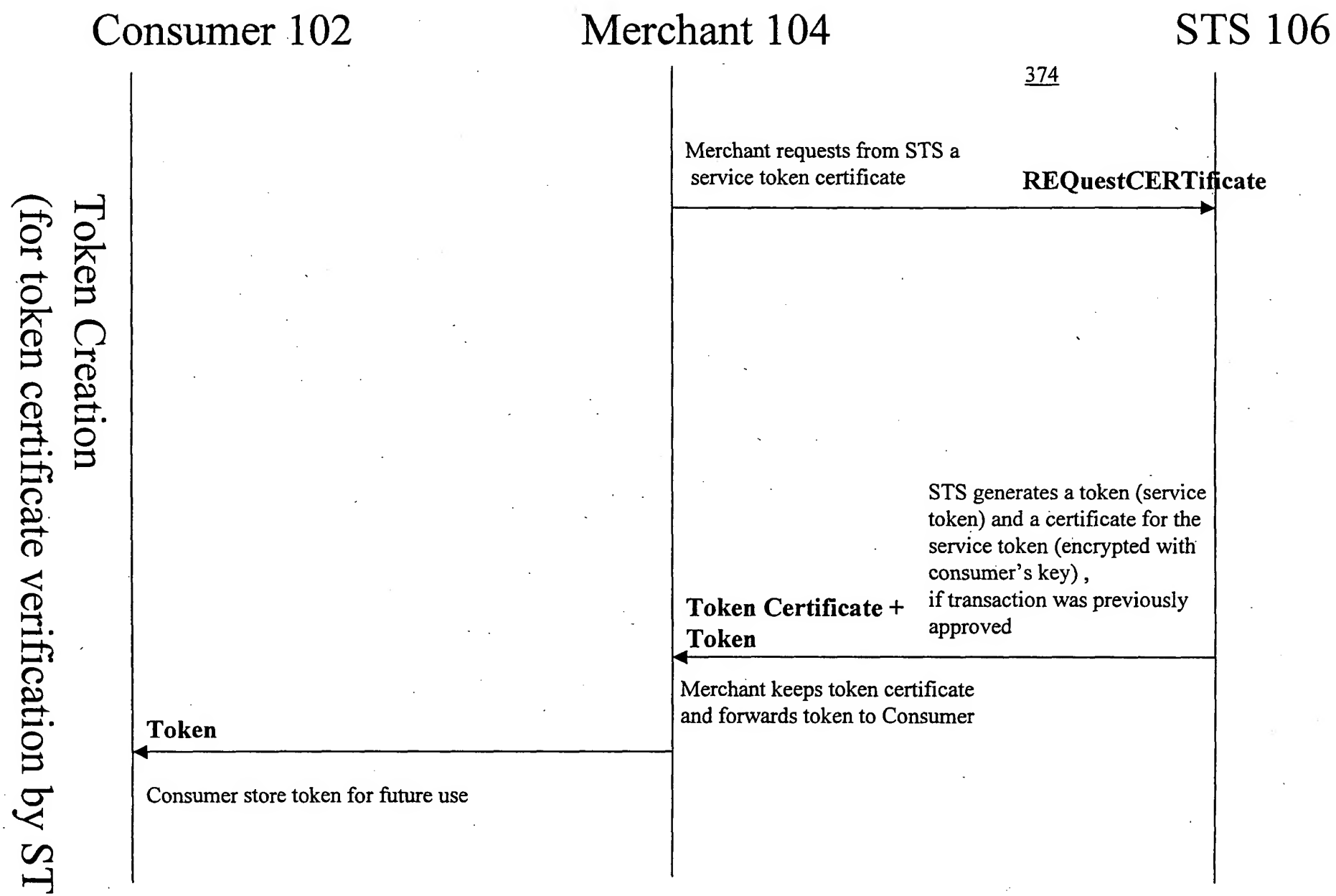

Consumer 102
Merchant 104
STS 106
374
Merchant requests from STS a service token certificate
REQuestCERTificate
STS generates a token (service token) and a certificate for the service token (encrypted with consumer's key) , if transaction was previously approved
Token Certificate + Token
Merchant keeps token certificate and forwards token to Consumer
Token
Consumer store token for future use
Token Creation
(for token certificate verification by STS)

Figure 25

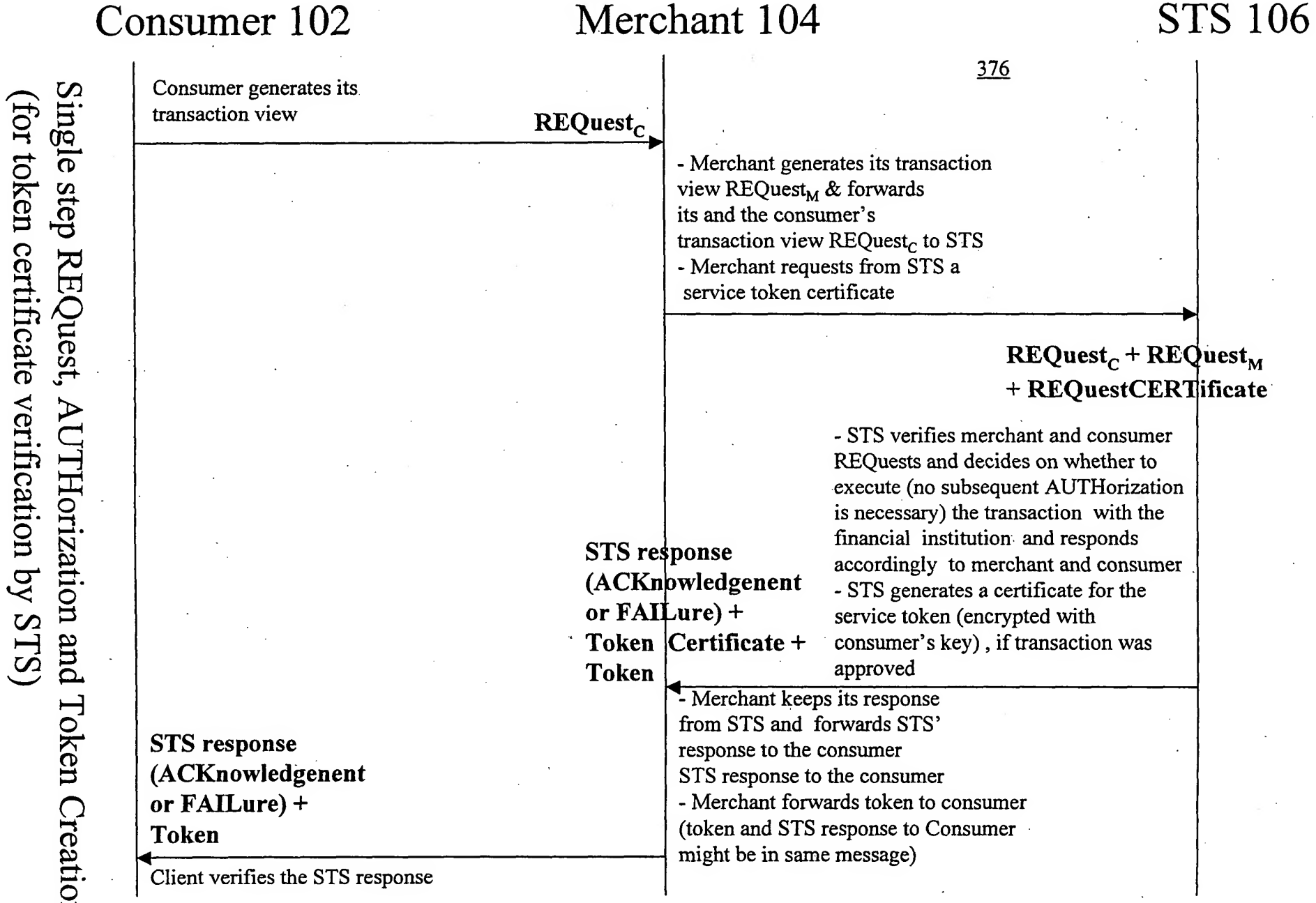

Consumer 102
Merchant 104
STS 106
Single step REQuest, AUTHorization and Token Creation
(for token certificate verification by STS)
376
Consumer generates its transaction view
REQuest$_C$
- Merchant generates its transaction view REQuest$_M$ & forwards its and the consumer's transaction view REQuest$_C$ to STS
- Merchant requests from STS a service token certificate
REQuest$_C$ + REQuest$_M$ + REQuestCERTificate
- STS verifies merchant and consumer REQuests and decides on whether to execute (no subsequent AUTHorization is necessary) the transaction with the financial institution and responds accordingly to merchant and consumer
- STS generates a certificate for the service token (encrypted with consumer's key), if transaction was approved
STS response (ACKnowledgenent or FAILure) + Token Certificate + Token
- Merchant keeps its response from STS and forwards STS' response to the consumer
STS response to the consumer
- Merchant forwards token to consumer (token and STS response to Consumer might be in same message)
STS response (ACKnowledgenent or FAILure) + Token
Client verifies the STS response

Figure 26

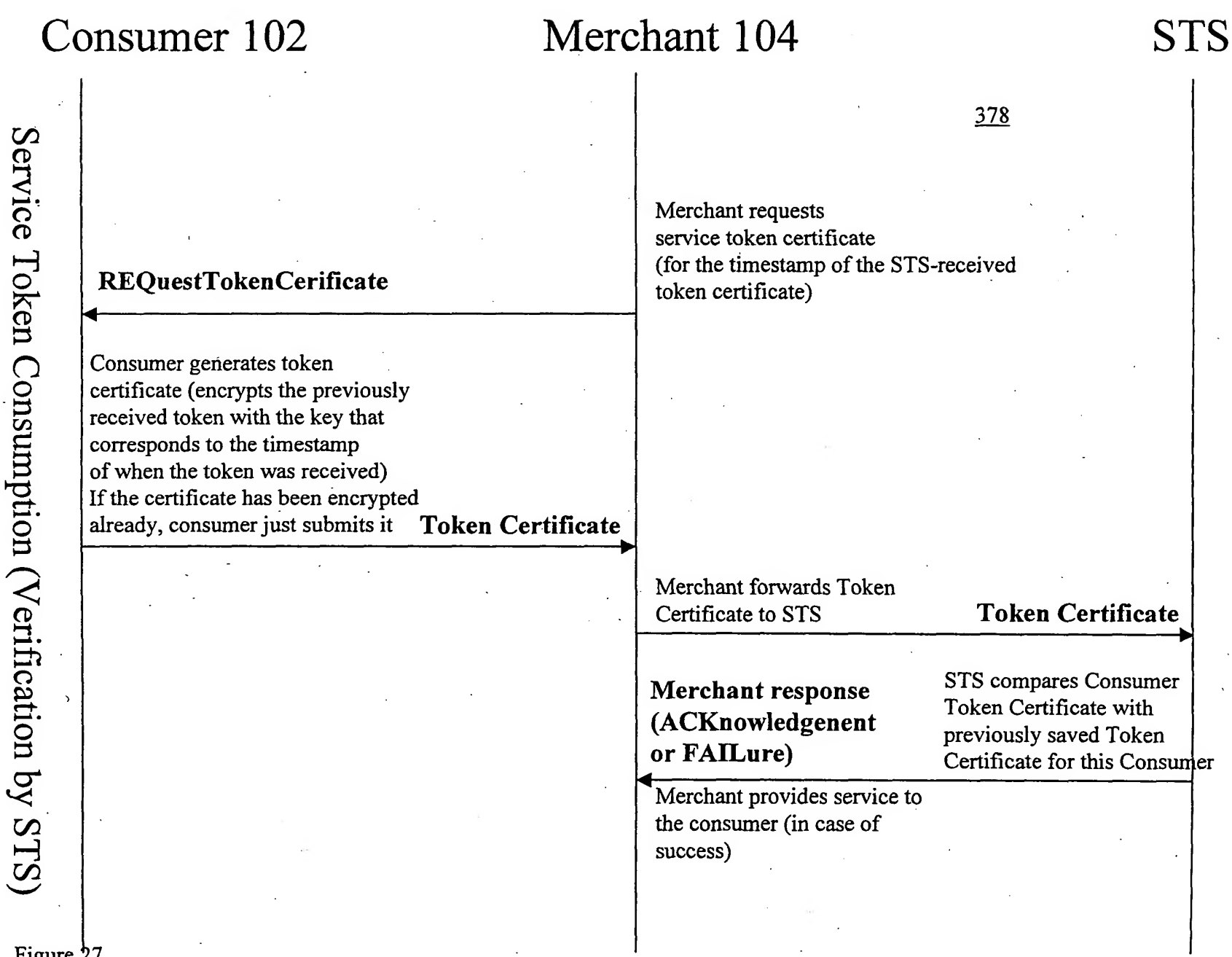

Consumer 102
Merchant 104
STS 106
Service Token Consumption (Verification by STS)
378
Merchant requests
service token certificate
(for the timestamp of the STS-received
token certificate)
REQuestTokenCerificate
Consumer generates token
certificate (encrypts the previously
received token with the key that
corresponds to the timestamp
of when the token was received)
If the certificate has been encrypted
already, consumer just submits it
Token Certificate
Merchant forwards Token
Certificate to STS
Token Certificate
Merchant response
(ACKnowledgenent
or FAILure)
STS compares Consumer
Token Certificate with
previously saved Token
Certificate for this Consumer
Merchant provides service to
the consumer (in case of
success)

Figure 27

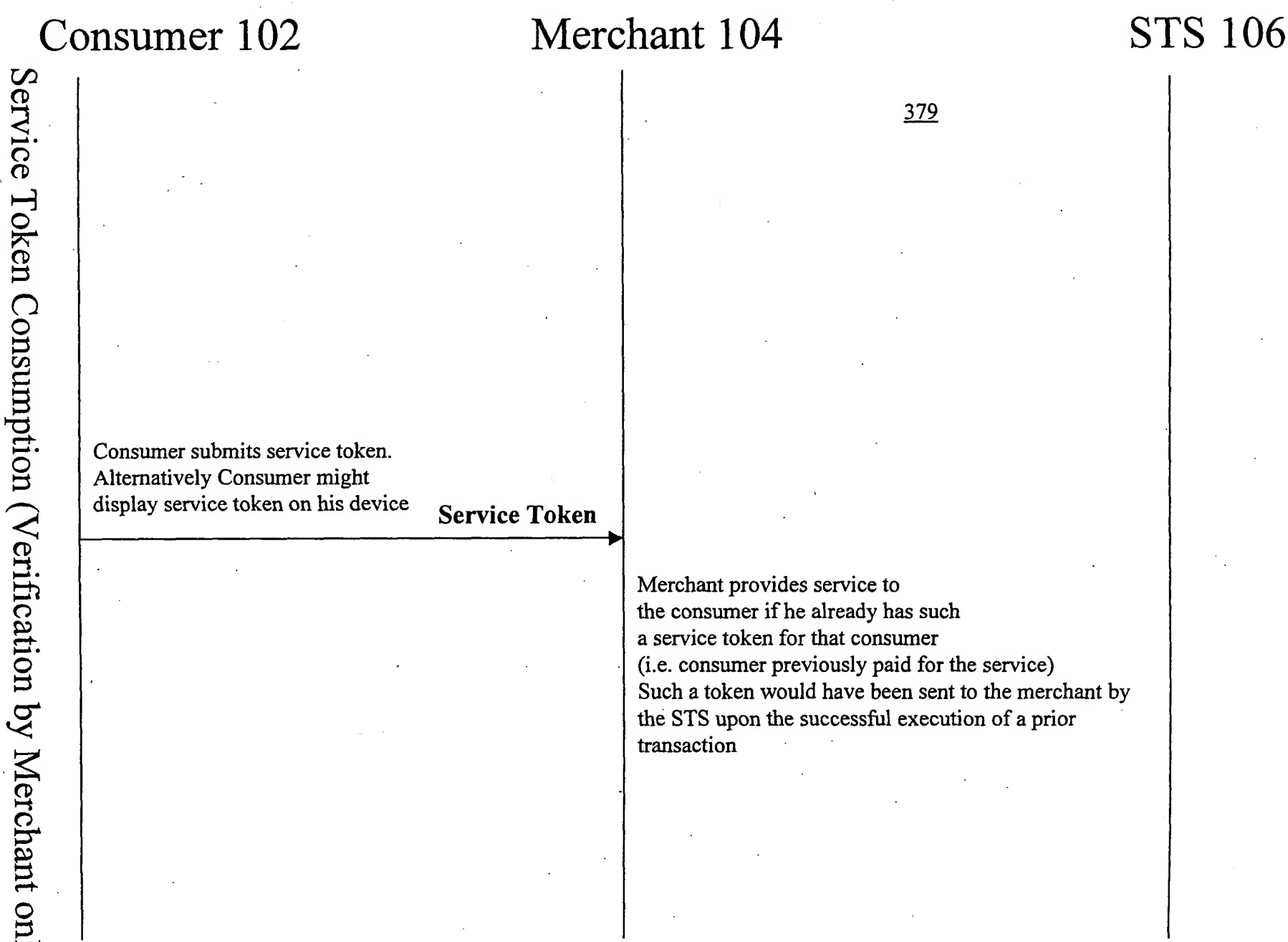

Consumer 102
Merchant 104
STS 106
Service Token Consumption (Verification by Merchant only)
379
Consumer submits service token.
Alternatively Consumer might
display service token on his device
Service Token
Merchant provides service to
the consumer if he already has such
a service token for that consumer
(i.e. consumer previously paid for the service)
Such a token would have been sent to the merchant by
the STS upon the successful execution of a prior
transaction

Figure 28

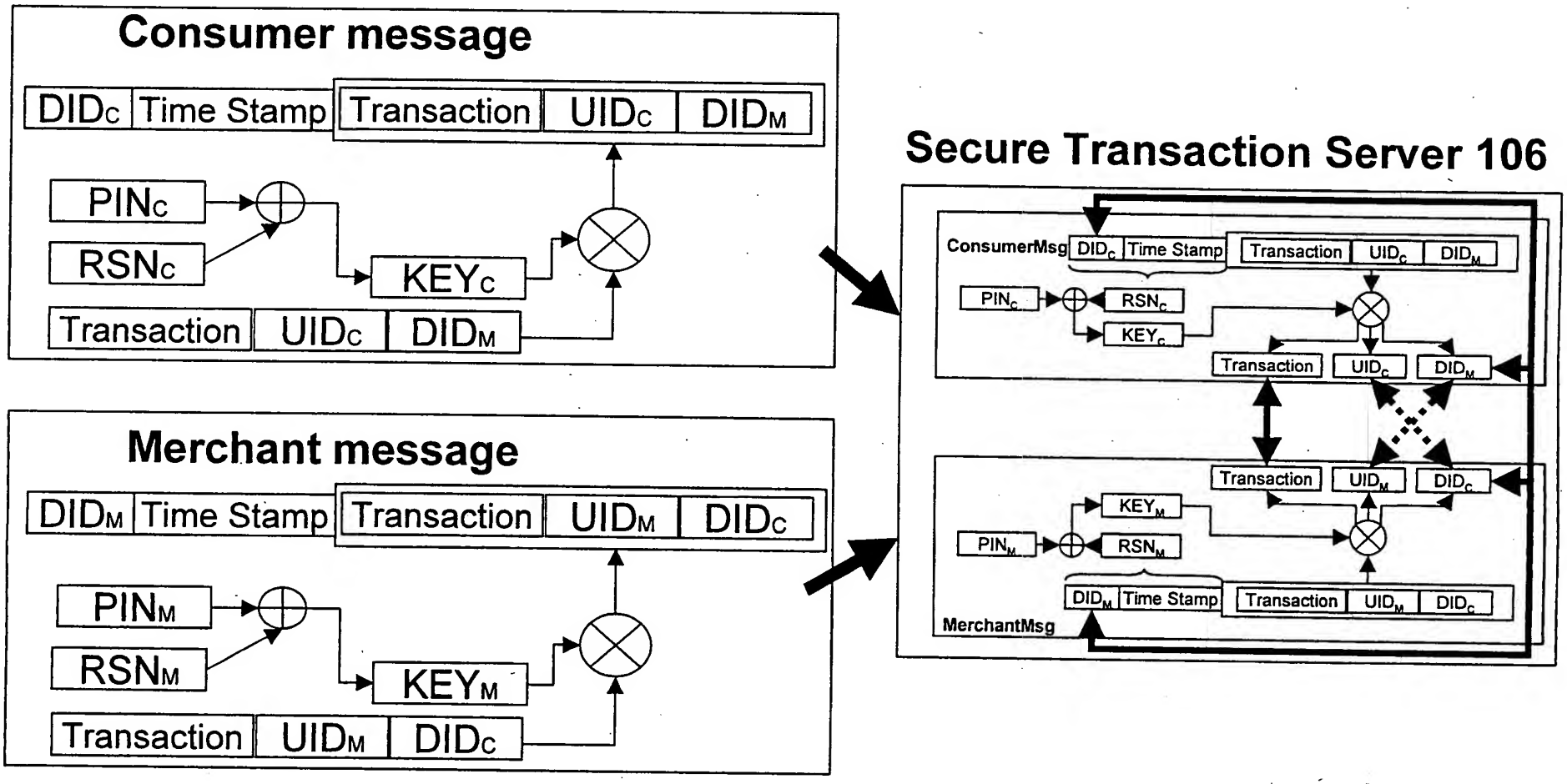

Consumer message
DIDC
Time Stamp
Transaction
UIDC
DIDM
PINC
RSNC
KEYC
Transaction
UIDC
DIDM
Merchant message
DIDM
Time Stamp
Transaction
UIDM
DIDC
PINM
RSNM
KEYM
Transaction
UIDM
DIDC
Secure Transaction Server 106
ConsumerMsg
DIDC
Time Stamp
Transaction
UIDC
DIDM
PINC
RSNC
KEYC
Transaction
UIDC
DIDM
Transaction
UIDM
DIDC
KEYM
PINM
RSNM
DIDM
Time Stamp
Transaction
UIDM
DIDC
MerchantMsg

Figure 29

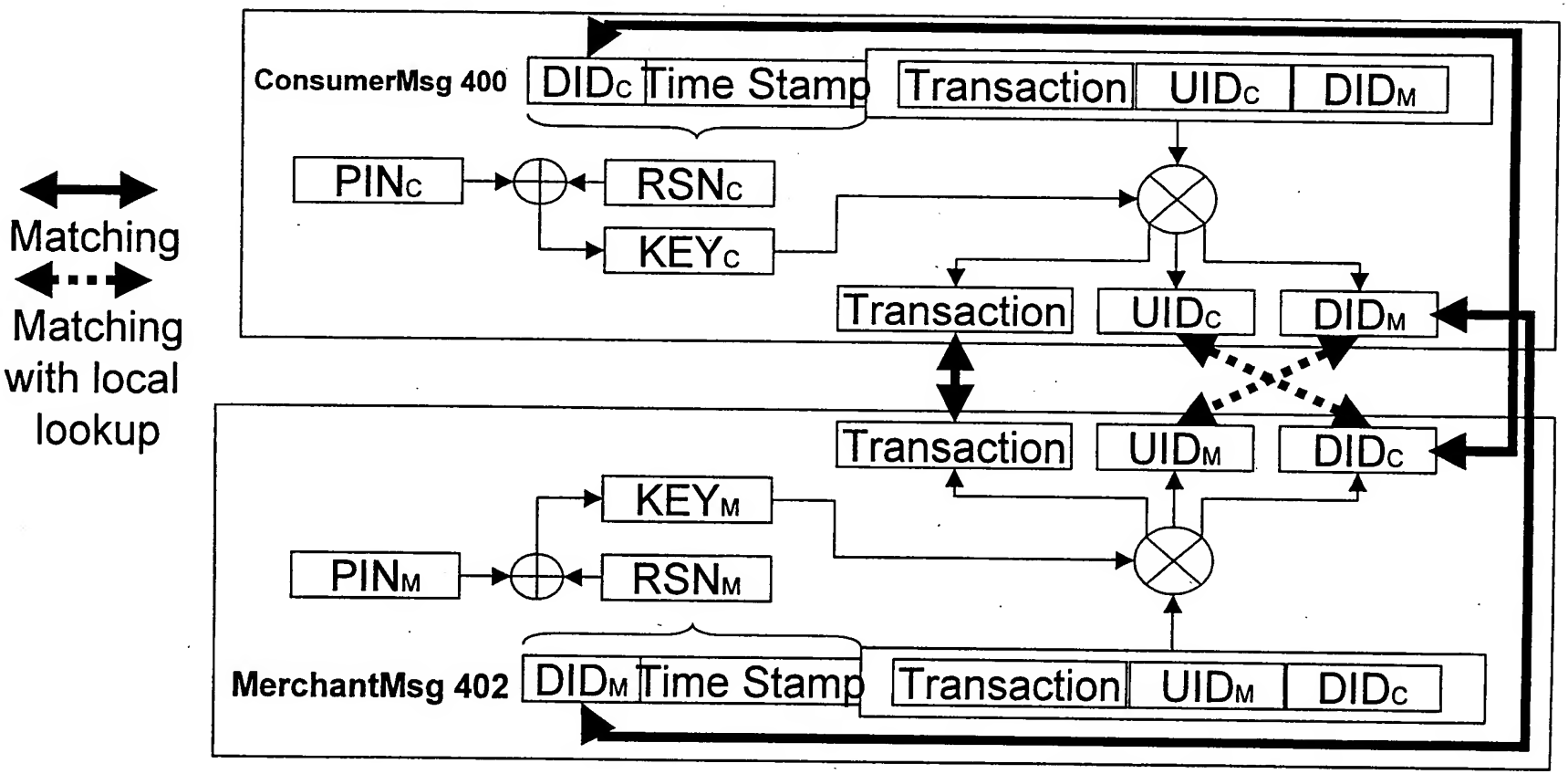

Matching
Matching with local lookup
ConsumerMsg 400
DIDC
Time Stamp
Transaction
UIDC
DIDM
PINC
RSNC
KEYC
Transaction
UIDC
DIDM
Transaction
UIDM
DIDC
KEYM
PINM
RSNM
MerchantMsg 402
DIDM
Time Stamp
Transaction
UIDM
DIDC

Figure 30

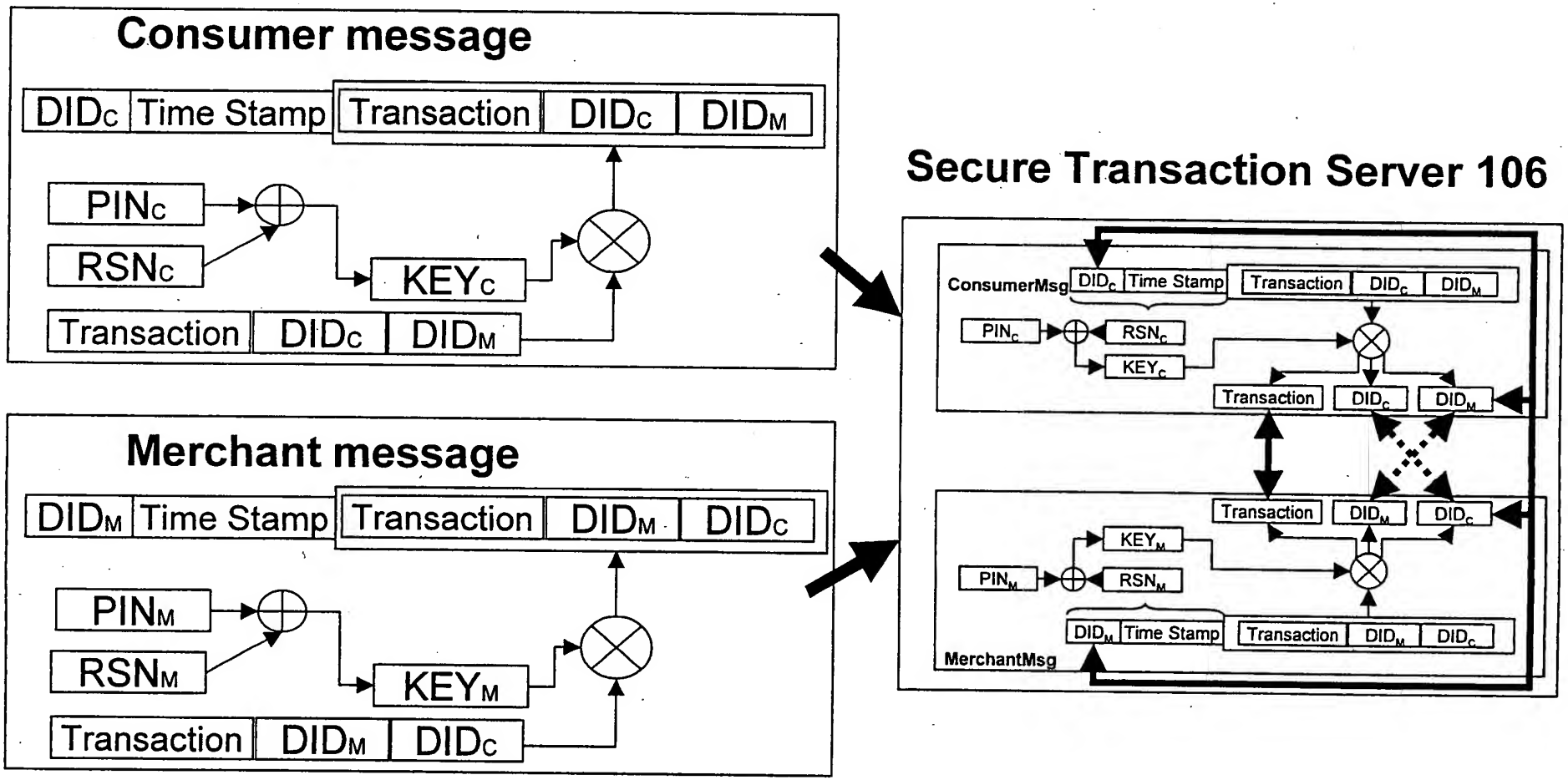

Consumer message
DIDC
Time Stamp
Transaction
DIDC
DIDM
PINC
RSNC
KEYC
Transaction
DIDC
DIDM
Merchant message
DIDM
Time Stamp
Transaction
DIDM
DIDC
PINM
RSNM
KEYM
Transaction
DIDM
DIDC
Secure Transaction Server 106
ConsumerMsg
DIDC
Time Stamp
Transaction
DIDC
DIDM
PINC
RSNC
KEYC
Transaction
DIDC
DIDM
Transaction
DIDM
DIDC
KEYM
PINM
RSNM
DIDM
Time Stamp
Transaction
DIDM
DIDC
MerchantMsg

Figure 31

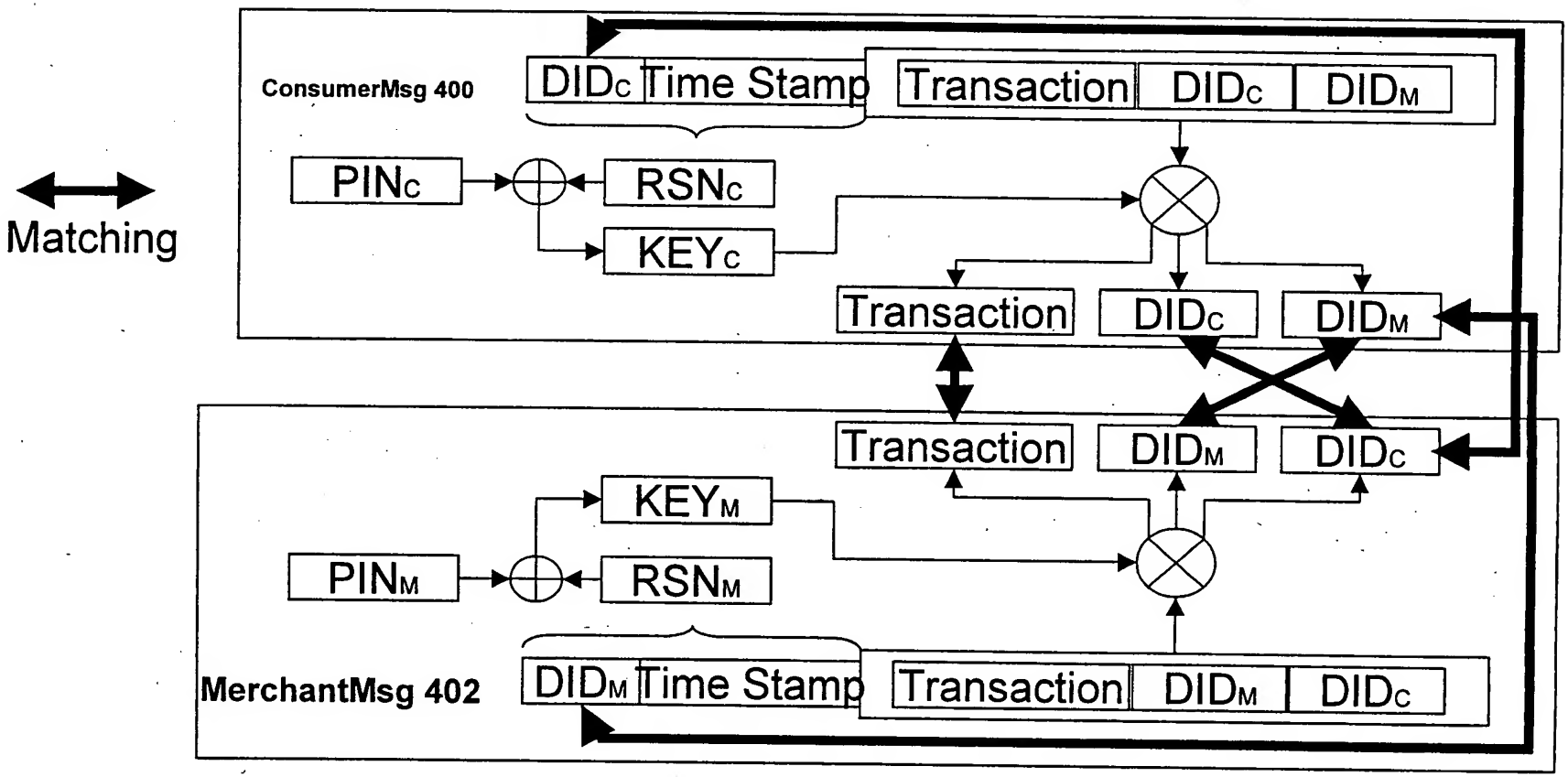

Matching
ConsumerMsg 400
DIDC Time Stamp
Transaction DIDC DIDM
PINC
RSNC
KEYC
Transaction DIDC DIDM
Transaction DIDM DIDC
KEYM
PINM
RSNM
MerchantMsg 402
DIDM Time Stamp
Transaction DIDM DIDC

Figure 32

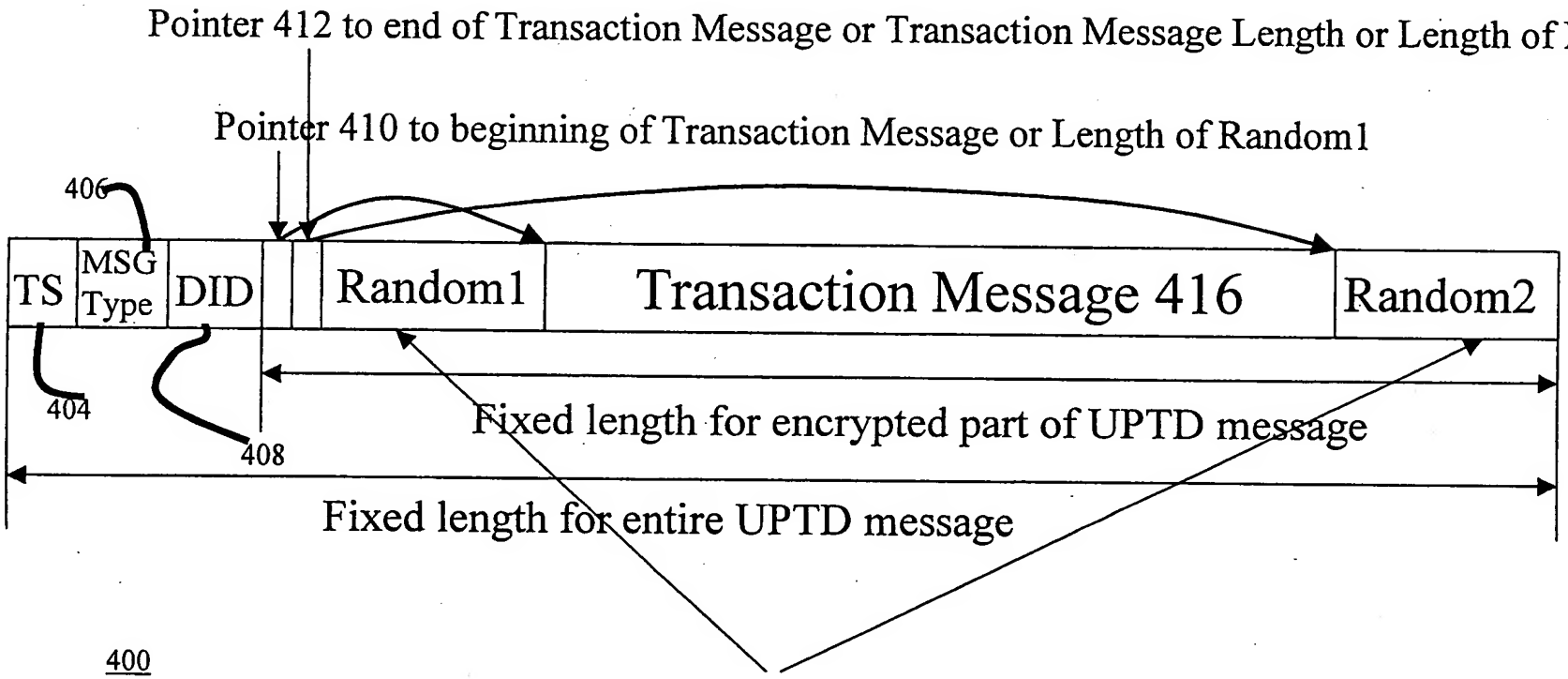
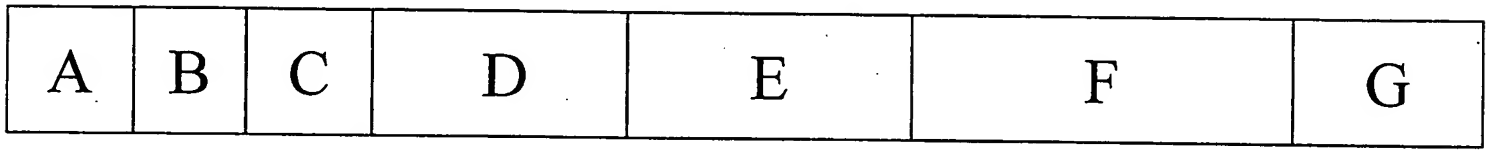

Pointer 412 to end of Transaction Message or Transaction Message Length or Length of Random2
Pointer 410 to beginning of Transaction Message or Length of Random1
406
TS
MSG Type
DID
Random1
Transaction Message 416
Random2
404
408
Fixed length for encrypted part of UPTD message
Fixed length for entire UPTD message
400
Length of each "Random" section is random and decided at the time of message composition.
414: Random 1
418: Random 2

Figure 33

420



A: Message type (REQuest or AUTHorization; REQuest in this case)

B: Success Code for response to this message

C: Failure Code for response to this message

D: DID of message sending device

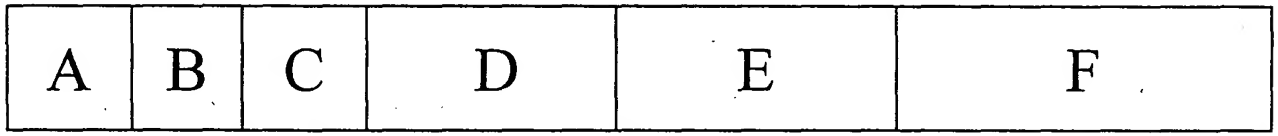
E: DID of other transacting party's device

F: Transaction amount or some other agreed transaction description

G: Friendly name of account to be used to pay D's user, amount E
F is optional and might be specified in AUTHorization message

Figure 34

422



A: Message type (REQuest or AUTHorization; REQuest in this case)

B: Success Code for response to this message

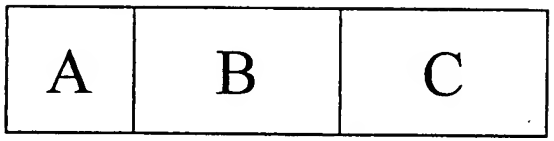
C: Failure Code for response to this message

D: DID of message sending device

E: DID of other transacting party's device

F: Transaction amount or some other agreed transaction description

Figure 35



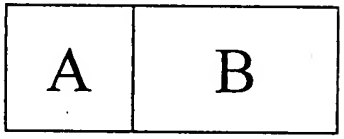
A: The Success or Failure code indicated by Payer depending on whether the REQuest was successful or not

B: A randomly generated number to be used to refer to the transaction for the remainder of the change

C: Payer's account listing

Figure 36

426

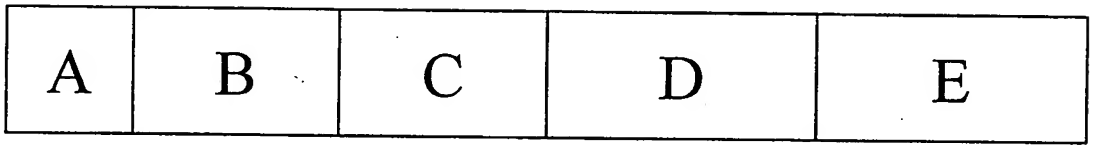


A: The Success or Failure code indicated by Payer depending on whether the REQuest was successful or not

B: A randomly generated number to be used to refer to the transaction for the remainder of the exchange

Figure 37

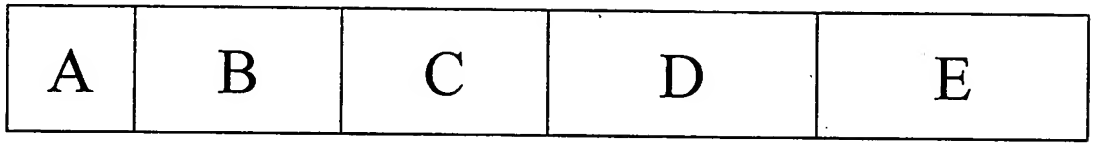
428



A: Message type (REQuest or AUTHorization; AUTHorization in this case)
B: Success Code for response to this message
C: Failure Code for response to this message
D: A reference to the transaction been authorized; a previously STS-generated reference is used
E: Optional to reference payer's account if not previously specified

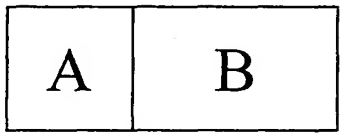
Figure 38

430



A: Message type (REQuest or AUTHorization; AUTHorization in this case)
B: Success Code for response to this message
C: Failure Code for response to this message
D: A reference to the transaction been authorized; a previously STS-generated reference is used
E: Optional to reference payee's account if not previously specified

Figure 39



A: The Success or Failure code indicated by Payer depending on whether the Authorization was successful or not

B: An optional additional description, for example a service token value (receipt)

Figure 40

434

A: The Success or Failure code indicated by Payee depending on whether the Authorization was successful or not

B: An optional additional description, for example a service token value (receipt)

Figure 41

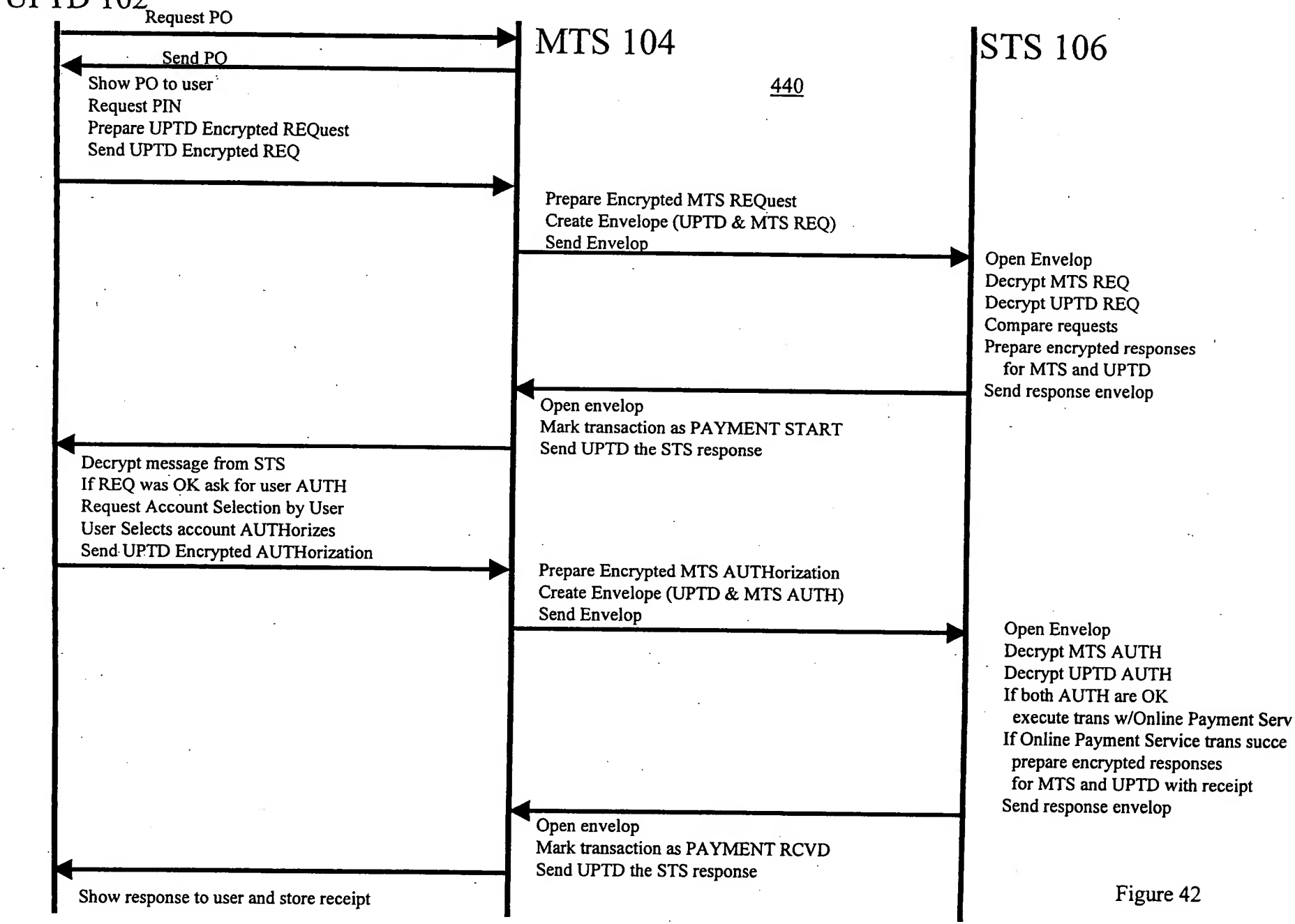

UPTD 102
MTS 104
STS 106
440
Request PO
Send PO
Show PO to user
Request PIN
Prepare UPTD Encrypted REQuest
Send UPTD Encrypted REQ
Prepare Encrypted MTS REQuest
Create Envelope (UPTD & MTS REQ)
Send Envelop
Open Envelop
Decrypt MTS REQ
Decrypt UPTD REQ
Compare requests
Prepare encrypted responses
for MTS and UPTD
Send response envelop
Open envelop
Mark transaction as PAYMENT START
Send UPTD the STS response
Decrypt message from STS
If REQ was OK ask for user AUTH
Request Account Selection by User
User Selects account AUTHorizes
Send UPTD Encrypted AUTHorization
Prepare Encrypted MTS AUTHorization
Create Envelope (UPTD & MTS AUTH)
Send Envelop
Open Envelop
Decrypt MTS AUTH
Decrypt UPTD AUTH
If both AUTH are OK
execute trans w/Online Payment Serv
If Online Payment Service trans succe
prepare encrypted responses
for MTS and UPTD with receipt
Send response envelop
Open envelop
Mark transaction as PAYMENT RCVD
Send UPTD the STS response
Show response to user and store receipt

Figure 42

1 Consumer Requests Purchase Order (PO)
2 Consumer Receives PO
3 Consumer REQuests transaction (consumer enters PIN)
4 MTS sends MTS REQ and consumer REQ
5 STS requests from Online Payment Service the account listing for consumer
6 STS receives Online Payment Service account listing
7 STS Sends response to REQ with accounts for consumer
8 MTS forwards STS response to REQ to consumer
9 Consumer AUTHorizes transaction (consumer selects account)
10 MTS sends MTS AUTH and consumer AUTH
11 STS sends transaction to Online Payment Service
12 STS receives Online Payment Service response
13 STS sends response to AUTH
14 MTS forward STS response to AUTH to consumer
(consumer sees notification of success on his display)

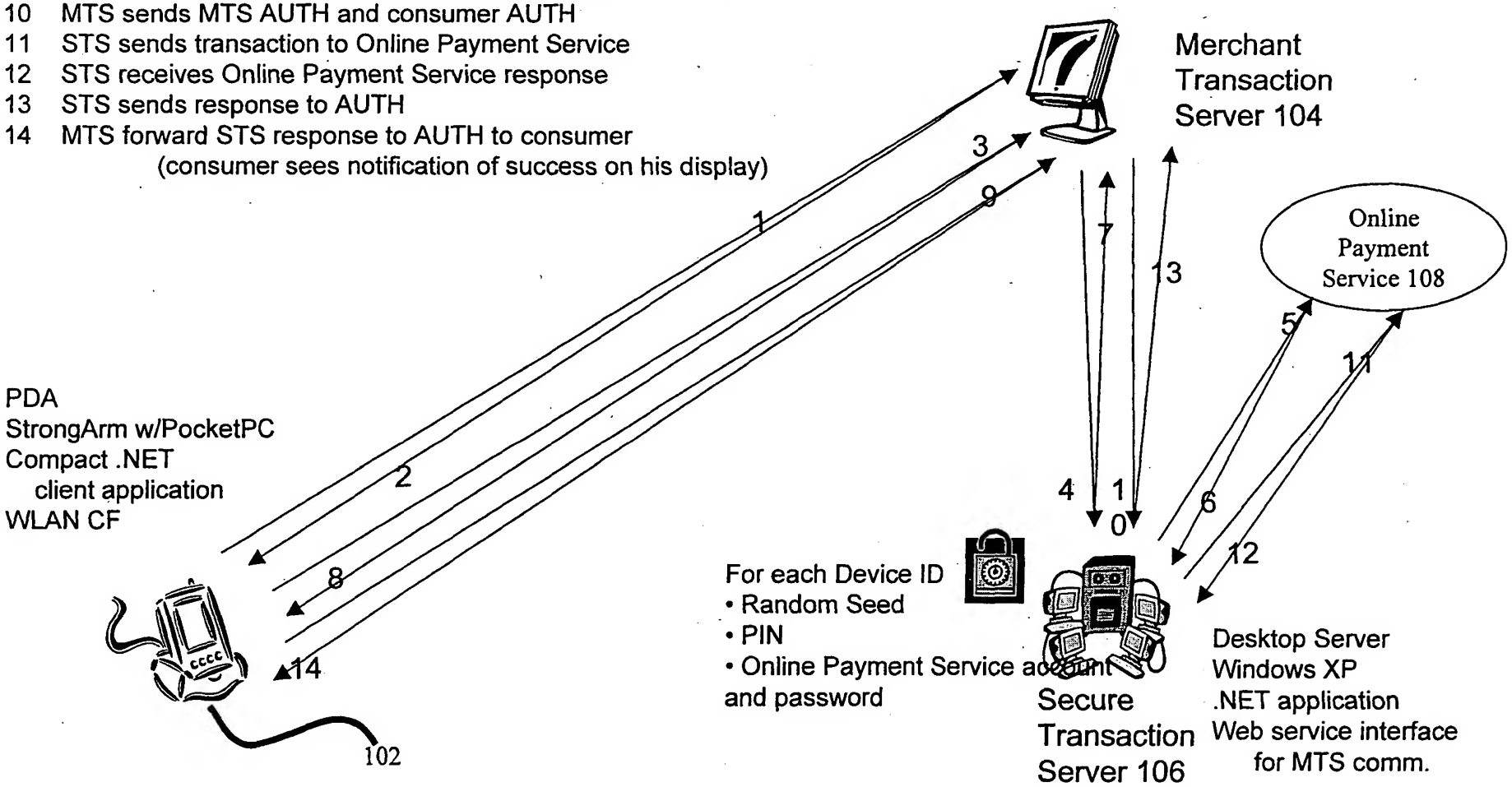


Figure 43

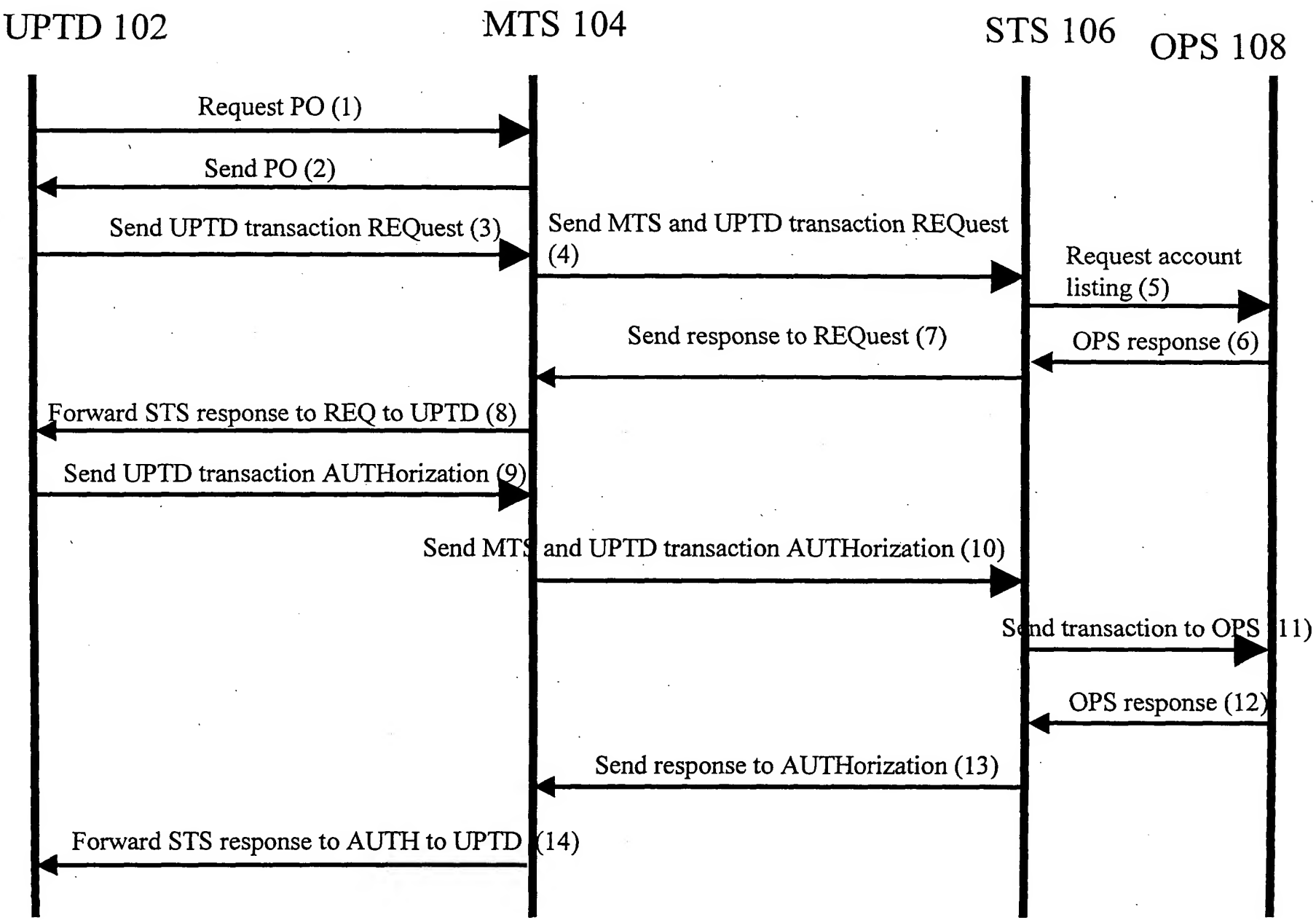

UPTD 102
MTS 104
STS 106
OPS 108
Request PO (1)
Send PO (2)
Send UPTD transaction REQuest (3)
Send MTS and UPTD transaction REQuest (4)
Request account listing (5)
OPS response (6)
Send response to REQuest (7)
Forward STS response to REQ to UPTD (8)
Send UPTD transaction AUTHorization (9)
Send MTS and UPTD transaction AUTHorization (10)
Send transaction to OPS (11)
OPS response (12)
Send response to AUTHorization (13)
Forward STS response to AUTH to UPTD (14)

Figure 44

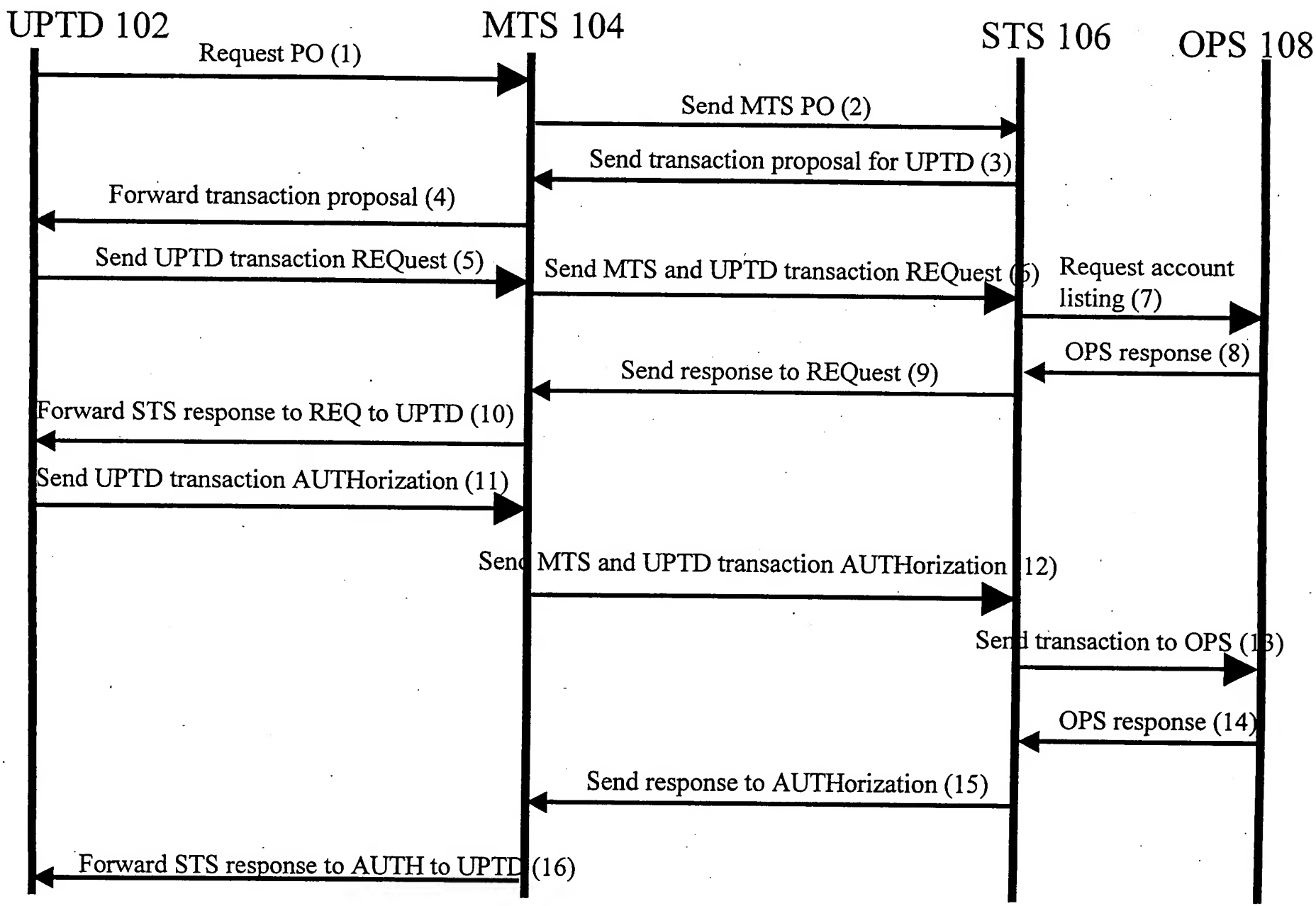

UPTD 102
MTS 104
STS 106
OPS 108
Request PO (1)
Send MTS PO (2)
Send transaction proposal for UPTD (3)
Forward transaction proposal (4)
Send UPTD transaction REQuest (5)
Send MTS and UPTD transaction REQuest (6)
Request account listing (7)
OPS response (8)
Send response to REQuest (9)
Forward STS response to REQ to UPTD (10)
Send UPTD transaction AUTHorization (11)
Send MTS and UPTD transaction AUTHorization (12)
Send transaction to OPS (13)
OPS response (14)
Send response to AUTHorization (15)
Forward STS response to AUTH to UPTD (16)

Figure 45

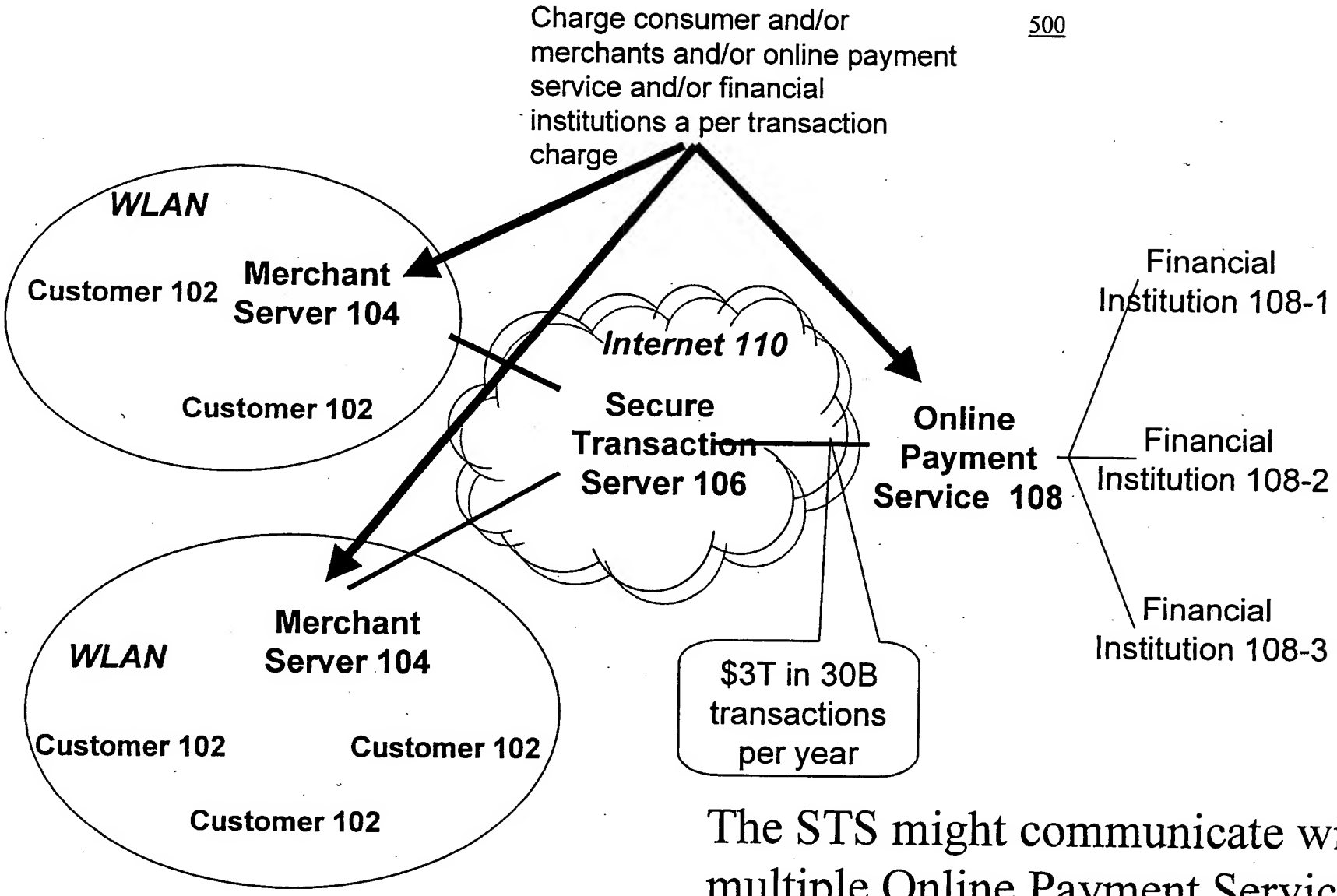

Charge consumer and/or merchants and/or online payment service and/or financial institutions a per transaction charge
500
WLAN
Customer 102
Merchant Server 104
Customer 102
Internet 110
Secure Transaction Server 106
Online Payment Service 108
Financial Institution 108-1
Financial Institution 108-2
Financial Institution 108-3
WLAN
Merchant Server 104
Customer 102
Customer 102
Customer 102
$3T in 30B transactions per year
The STS might communicate with multiple Online Payment Services

Figure 46

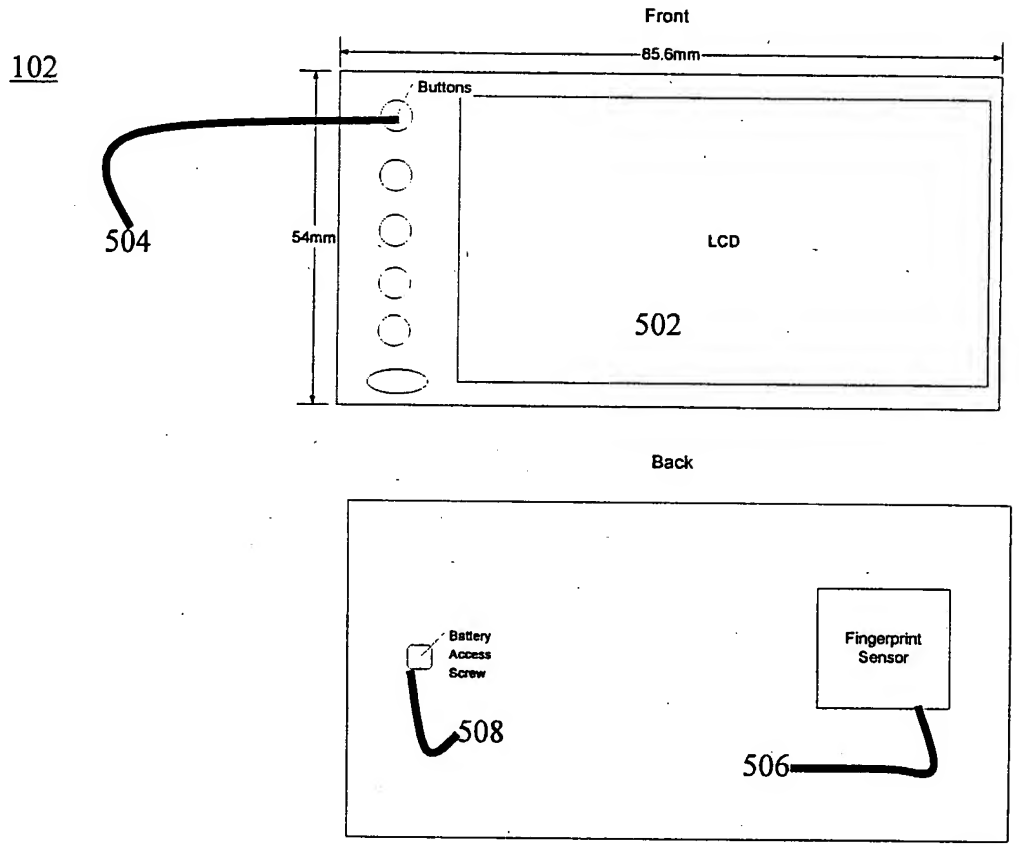

102
Front
85.6mm
Buttons
504
54mm
LCD
502
Back
Battery
Access
Screw
508
Fingerprint
Sensor
506

Figure 47

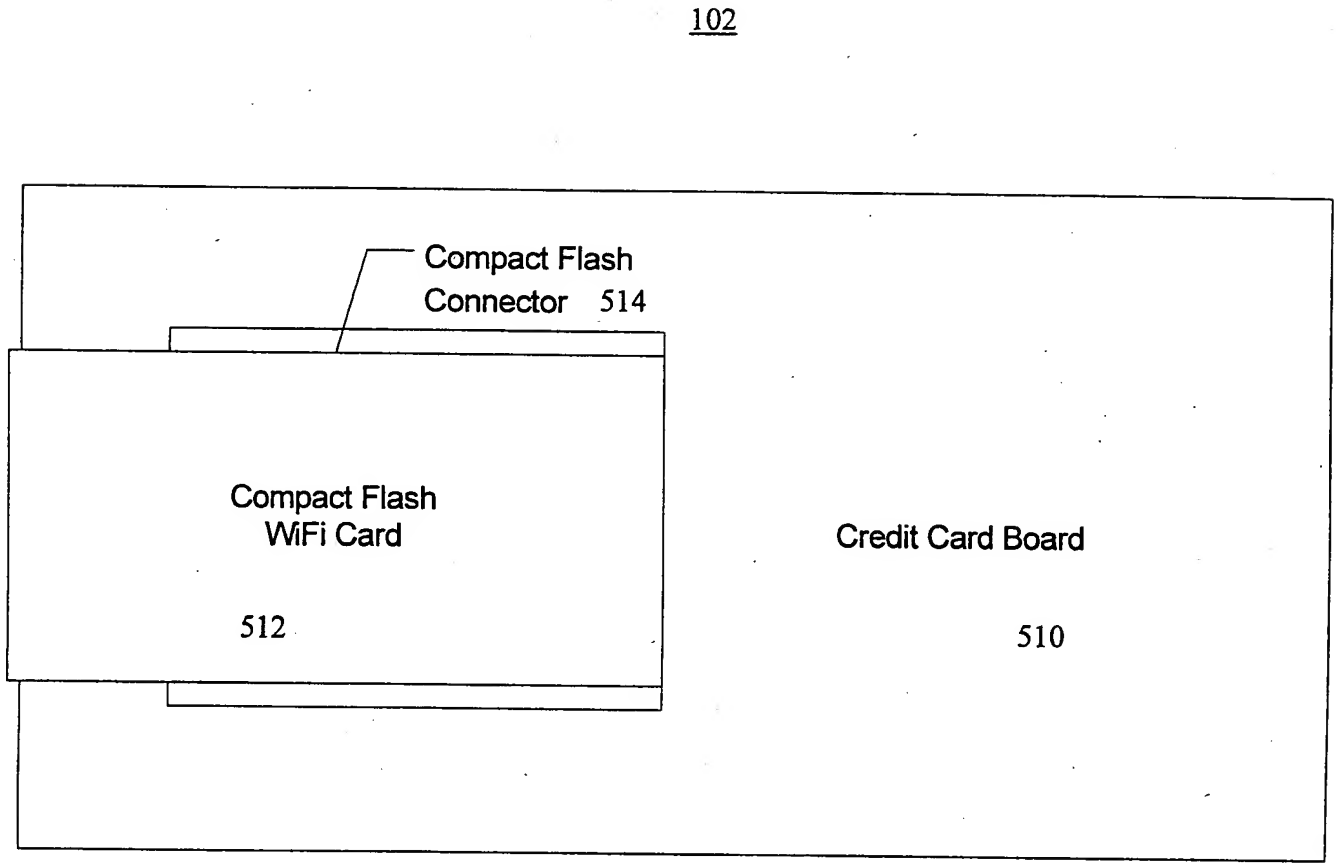

102
Compact Flash
Connector 514
Compact Flash
WiFi Card
512
Credit Card Board
510

Figure 48

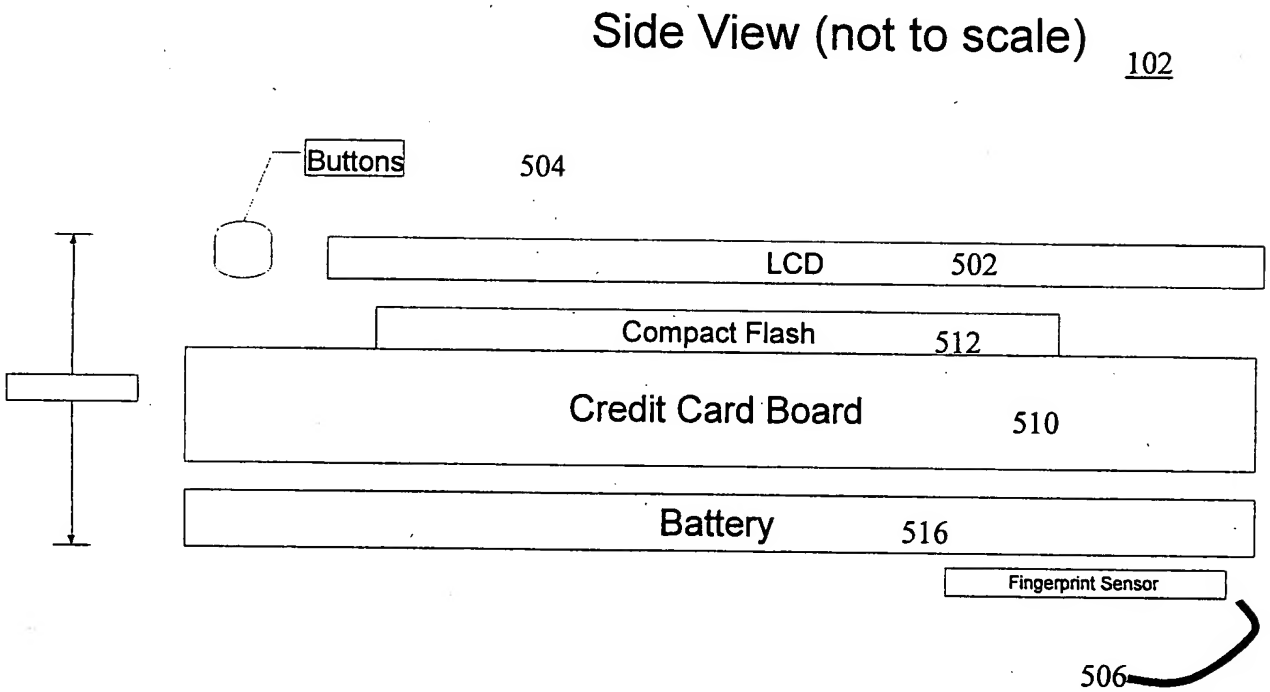

Side View (not to scale)
102
Buttons
504
LCD
502
Compact Flash
512
Credit Card Board
510
Battery
516
Fingerprint Sensor
506

Figure 49

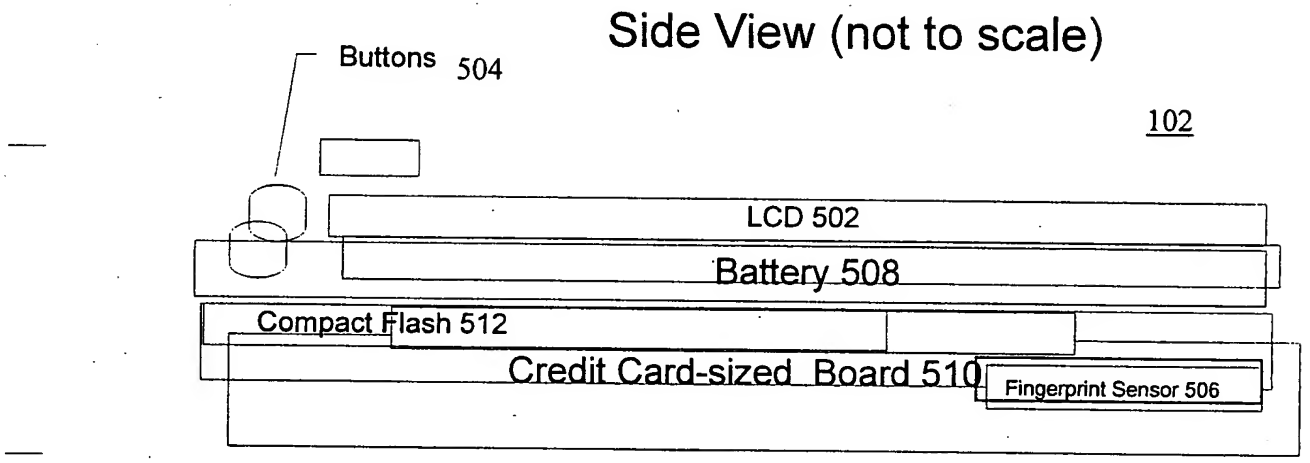

Side View (not to scale)
Buttons 504
102
LCD 502
Battery 508
Compact Flash 512
Credit Card-sized Board 510
Fingerprint Sensor 506

Figure 50

Pre-purchasing phase, example 600

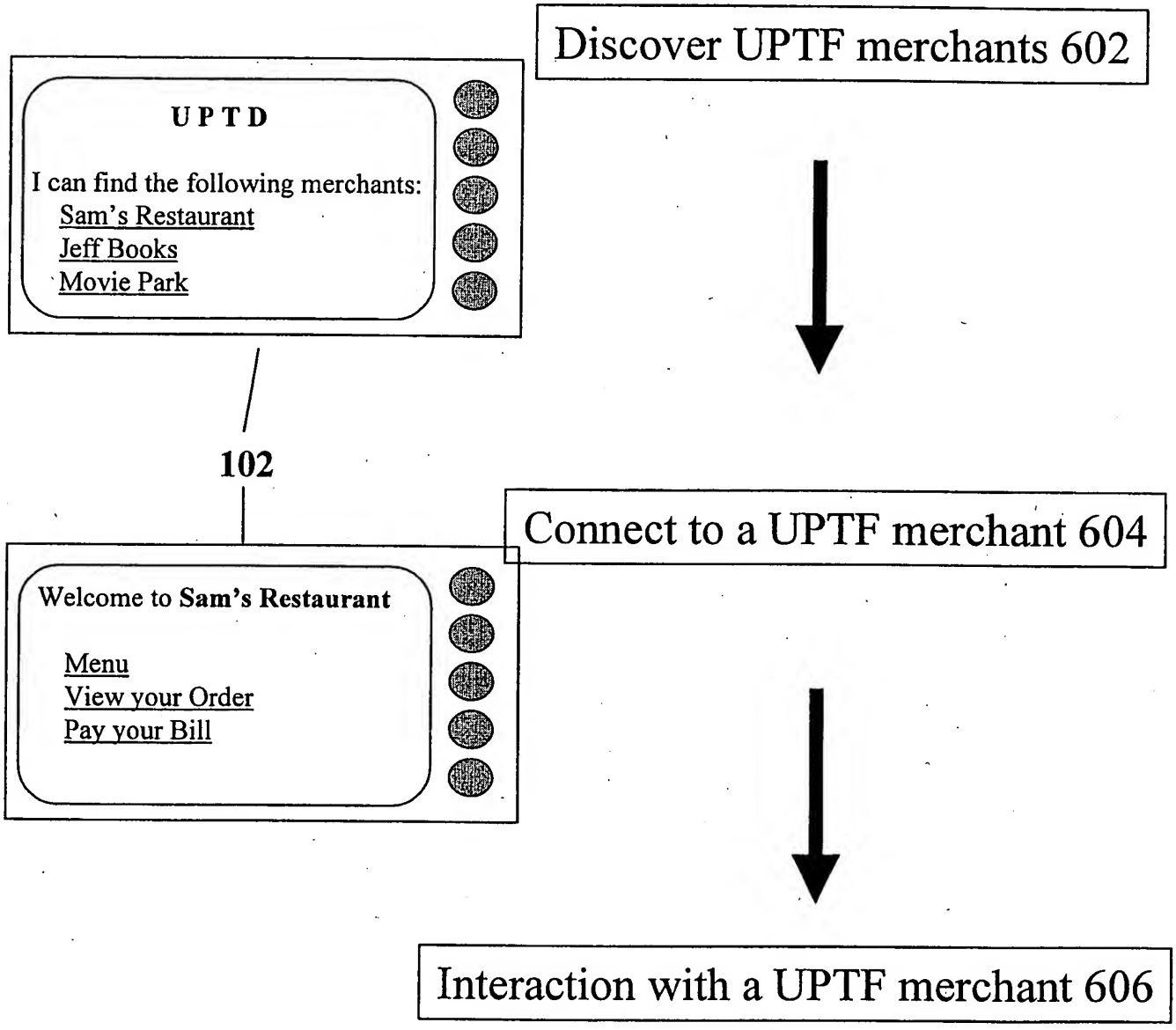


Figure 51

Physical Goods Purchase I, example 610

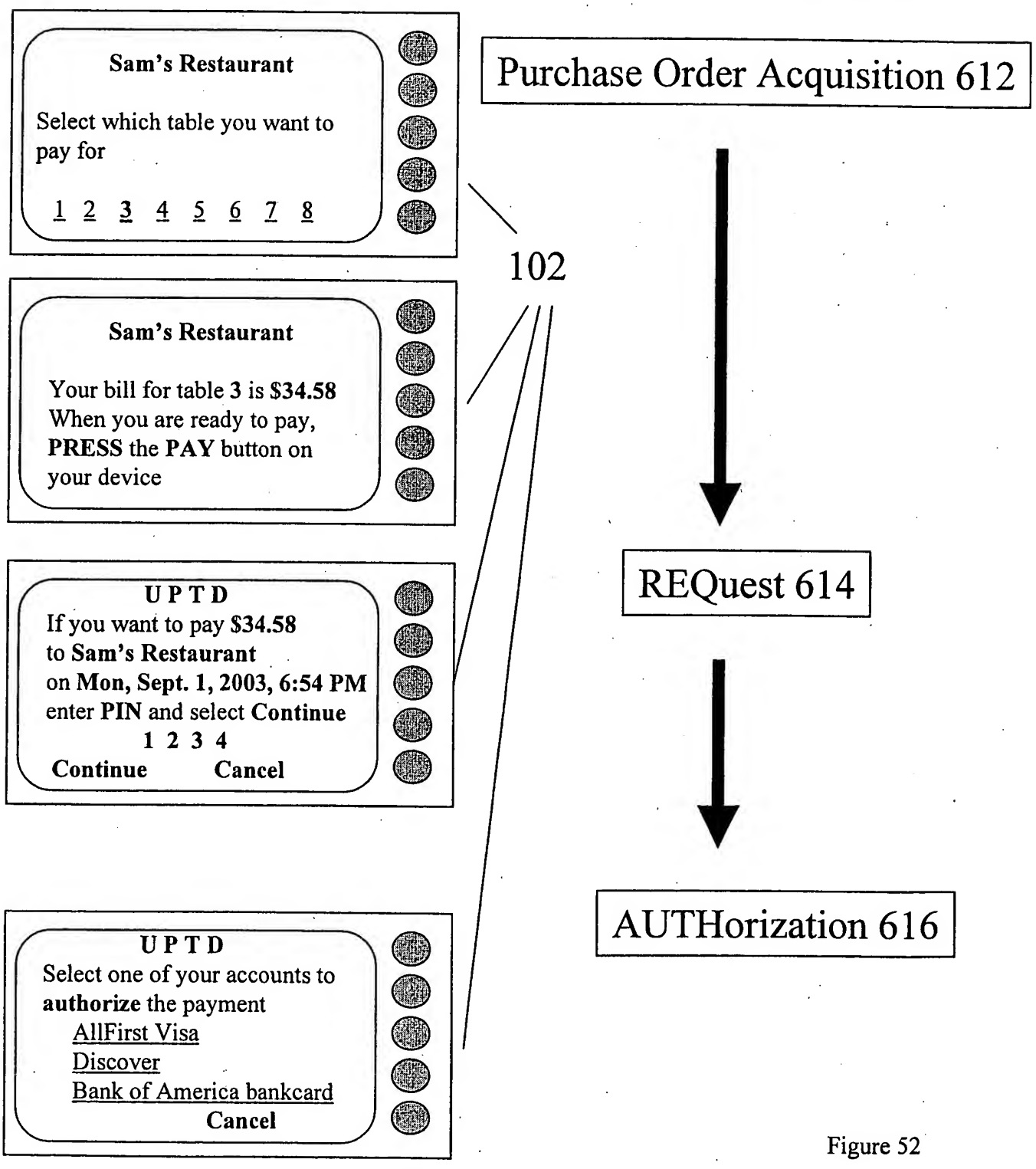


Figure 52

Physical Goods Purchase I, example, variation 620

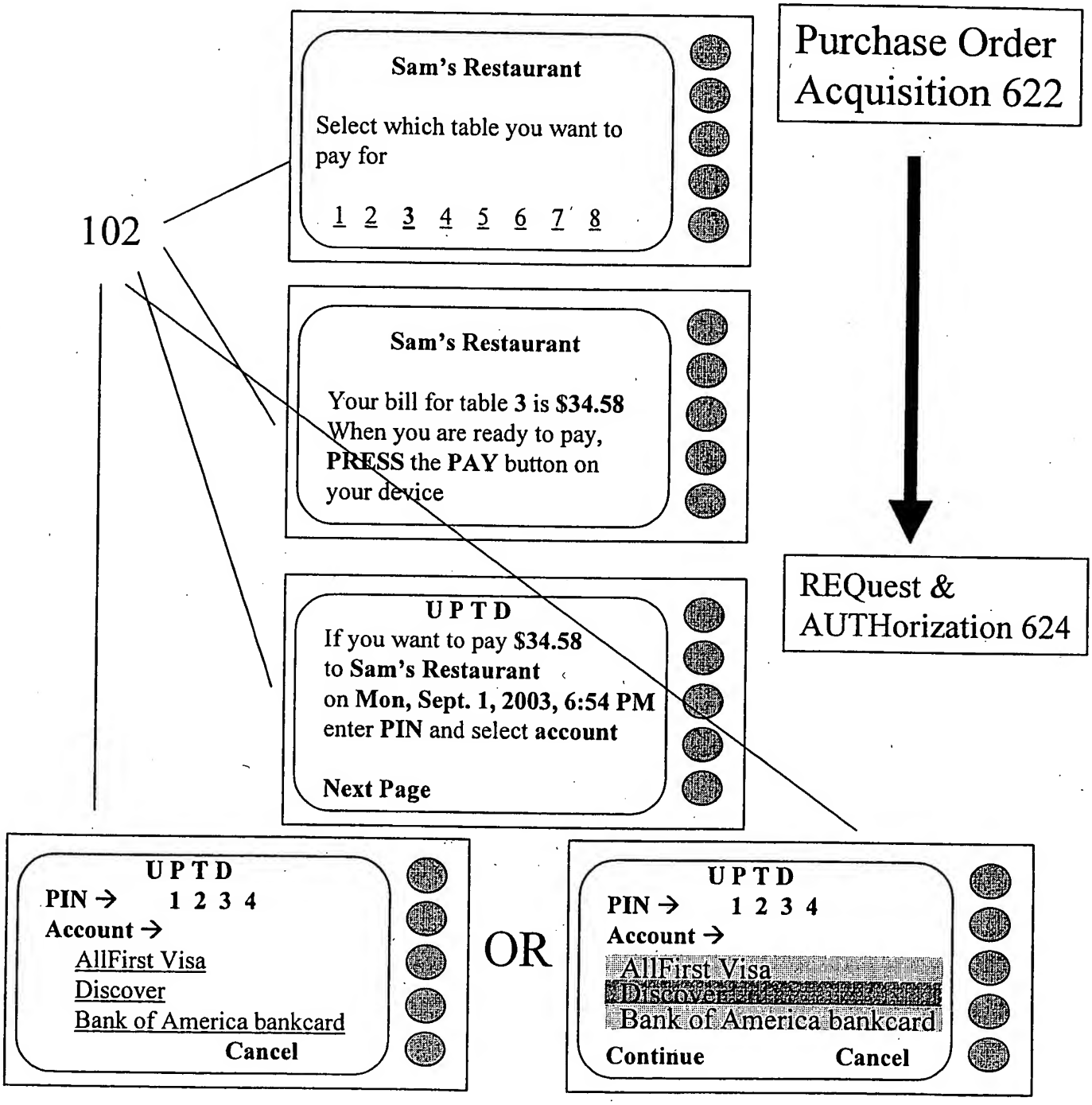


Figure 53

Physical Goods Purchase II, example 630

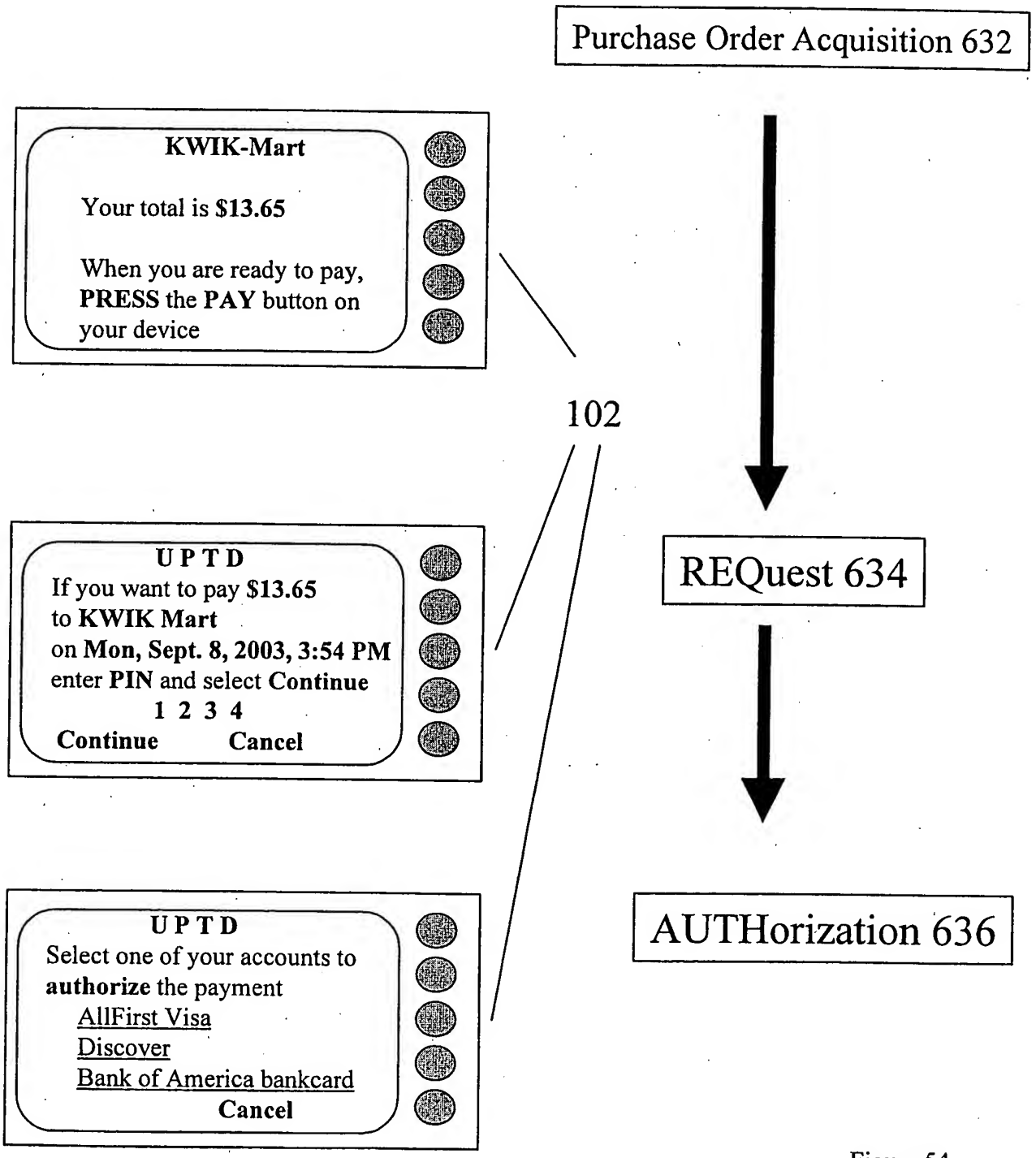


Figure 54

Service Purchase I, example 638

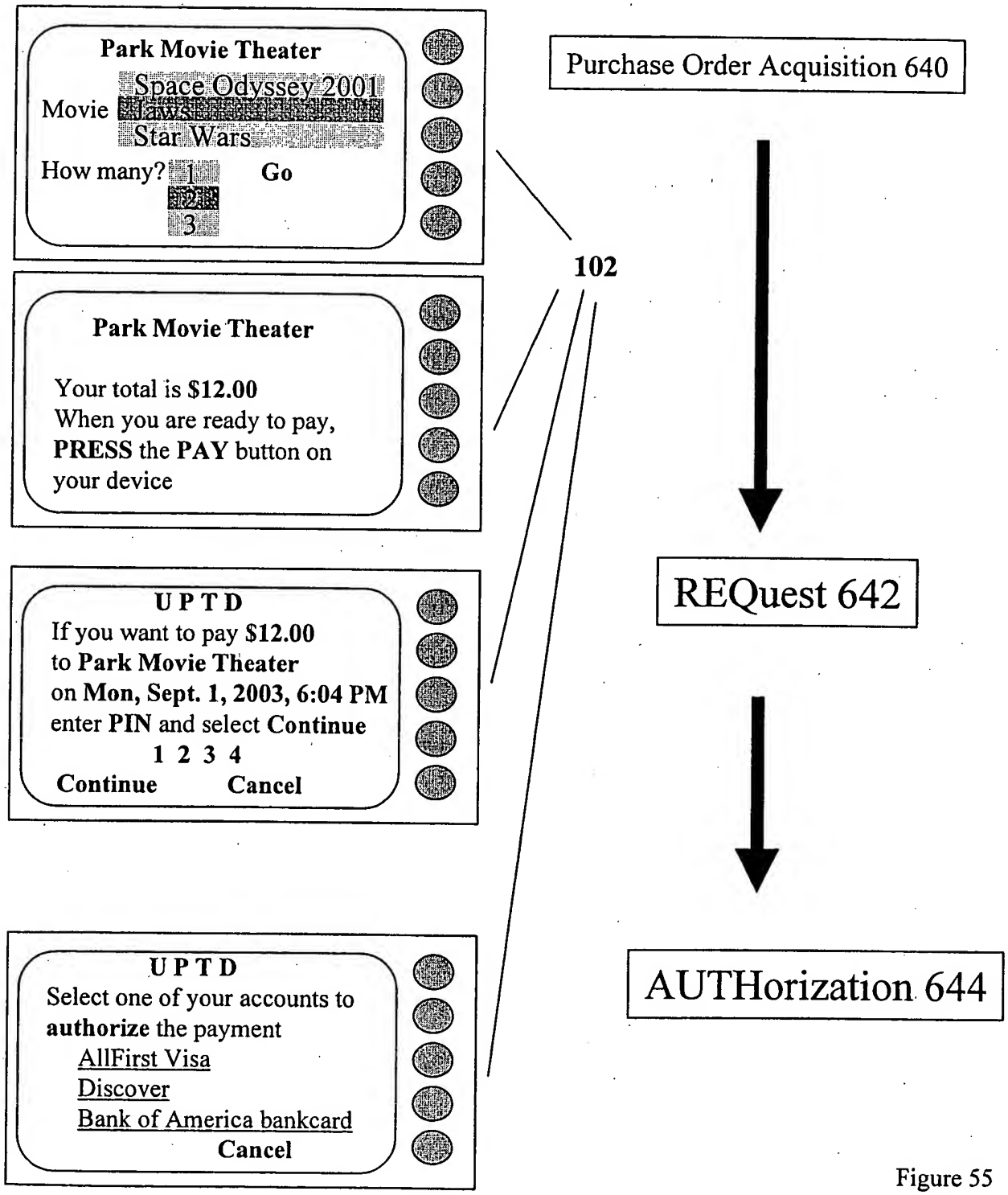


Figure 55

Service Purchase I – token verification and consumption, example 650

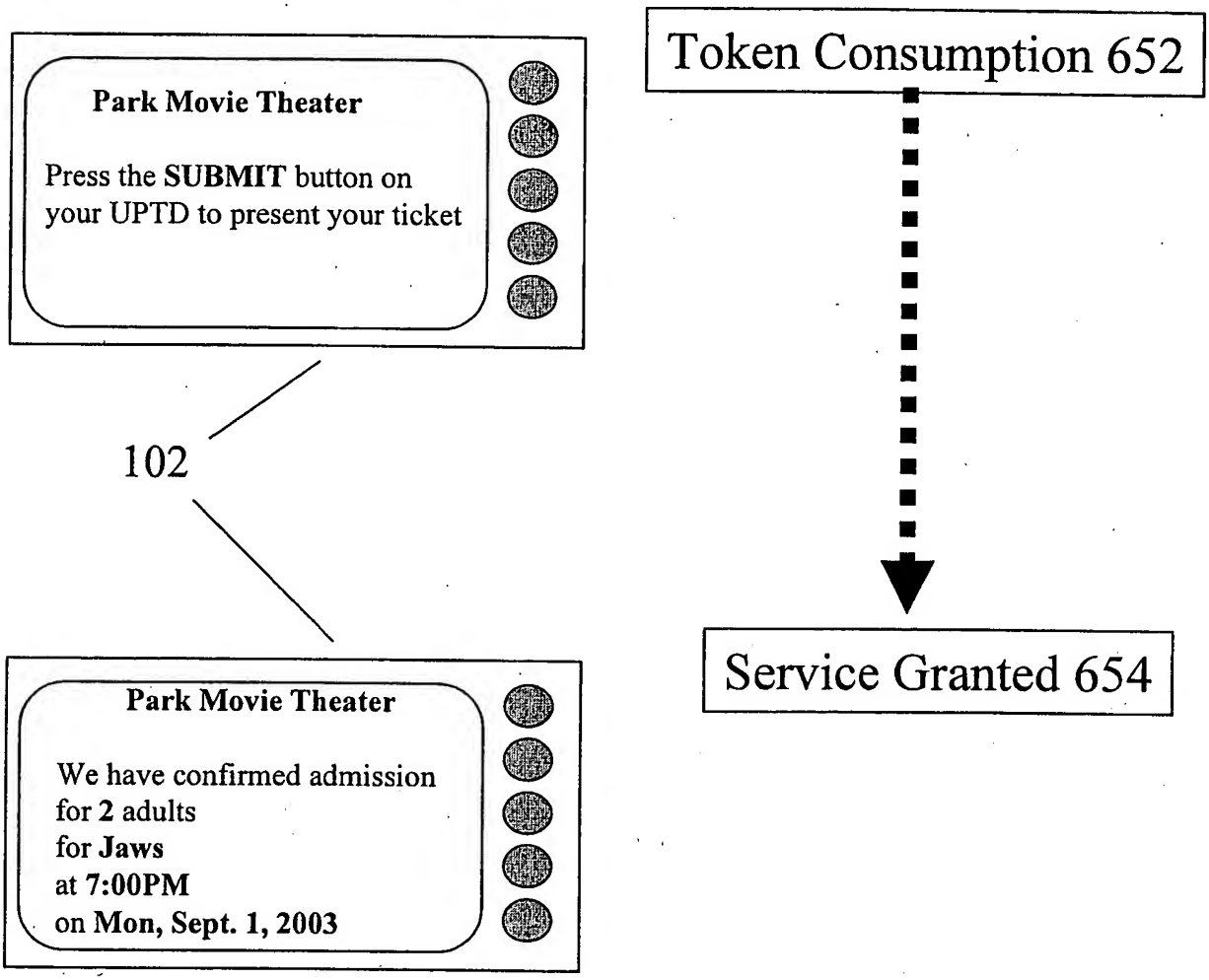


Figure 56

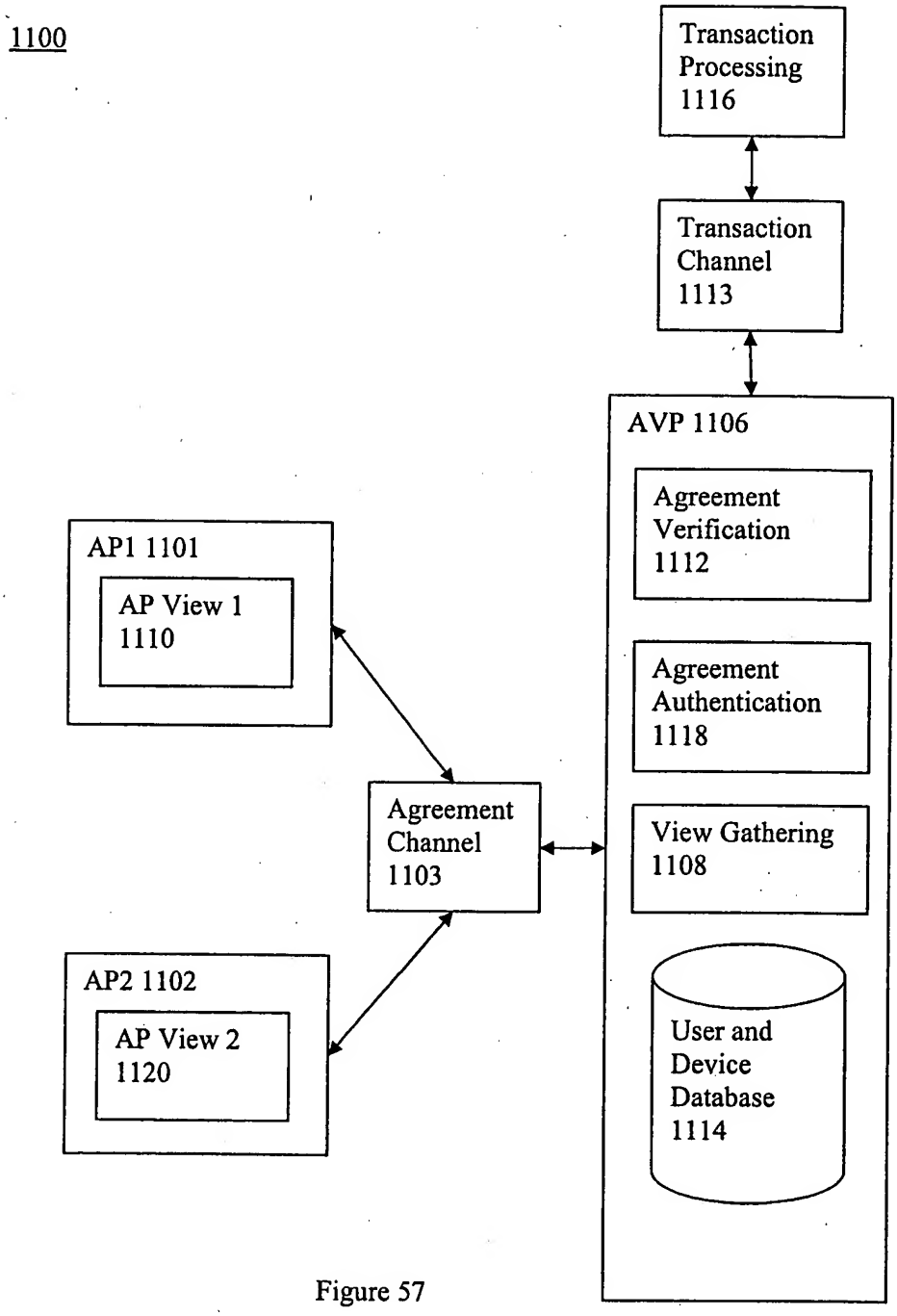

1100
Transaction Processing 1116
Transaction Channel 1113
AVP 1106
Agreement Verification 1112
Agreement Authentication 1118
View Gathering 1108
User and Device Database 1114
AP1 1101
AP View 1 1110
AP2 1102
AP View 2 1120
Agreement Channel 1103

Figure 57

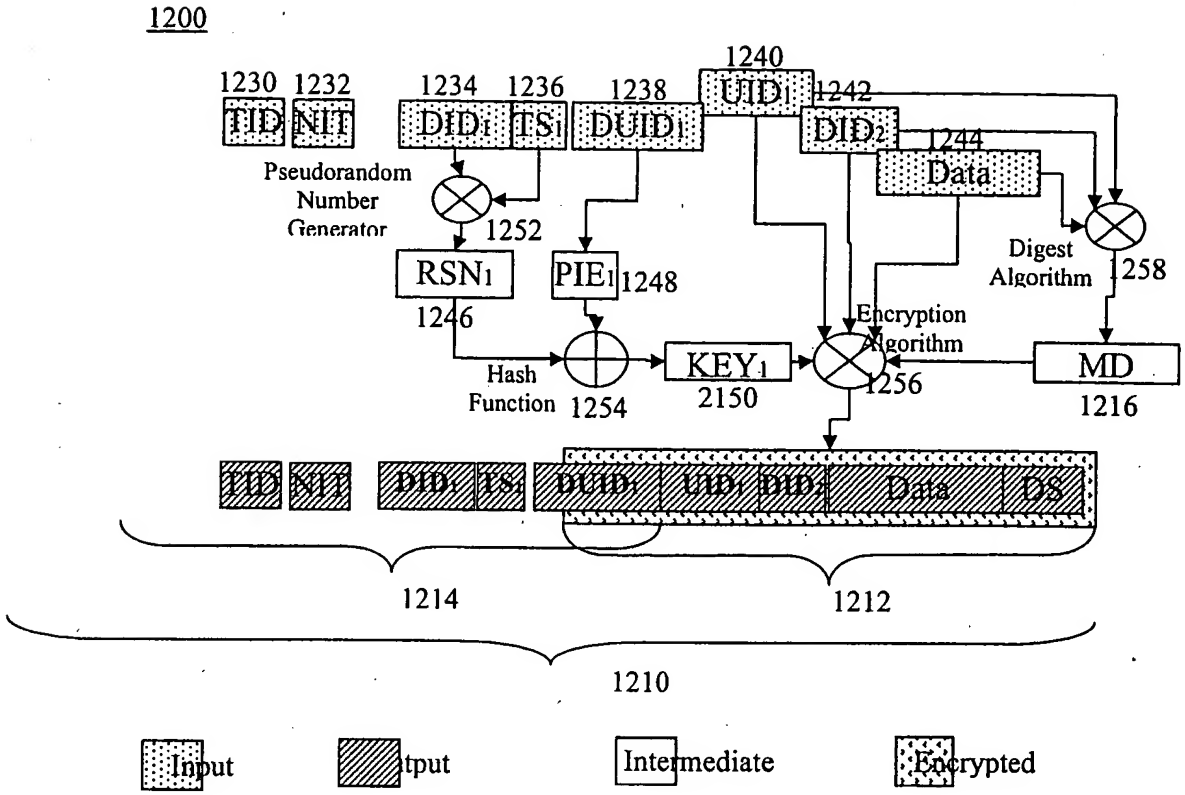

1200
1230
1232
1234
1236
1238
1240
1242
1244
TID
NIT
DID1
TS1
DUID1
UID1
DID2
Data
Pseudorandom Number Generator
1252
RSN1
PIE1
1248
1246
Hash Function
1254
KEY1
2150
Encryption Algorithm
1256
Digest Algorithm
1258
MD
1216
TID
NIT
DID1
TS1
DUID1
UID1
DID2
Data
DS
1214
1212
1210
Input
tput
Intermediate
Encrypted

Figure 58

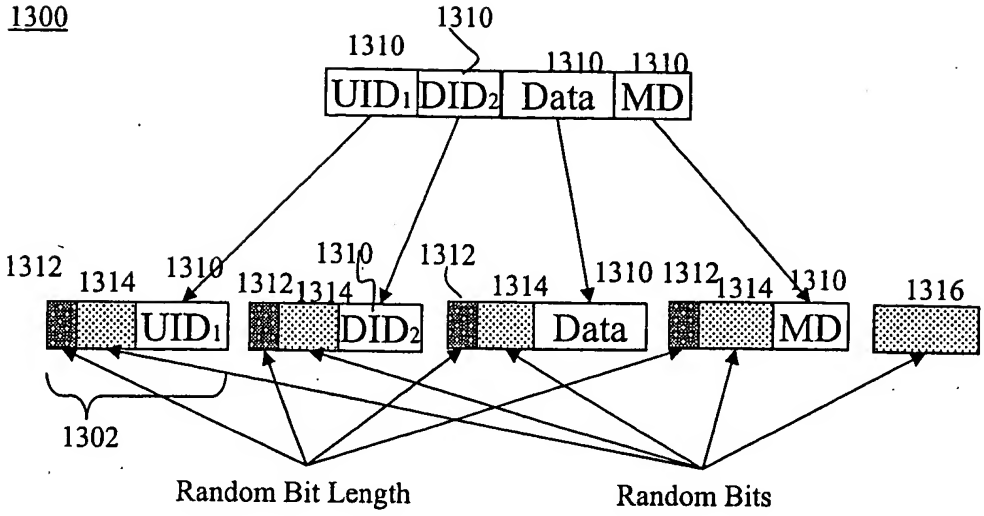

1300
1310
1310
1310
1310
UID1
DID2
Data
MD
1312
1314
1310
1310
1312
1312
1314
1314
1310
1312
1314
1310
1316
UID1
DID2
Data
MD
1302
Random Bit Length
Random Bits

Figure 59

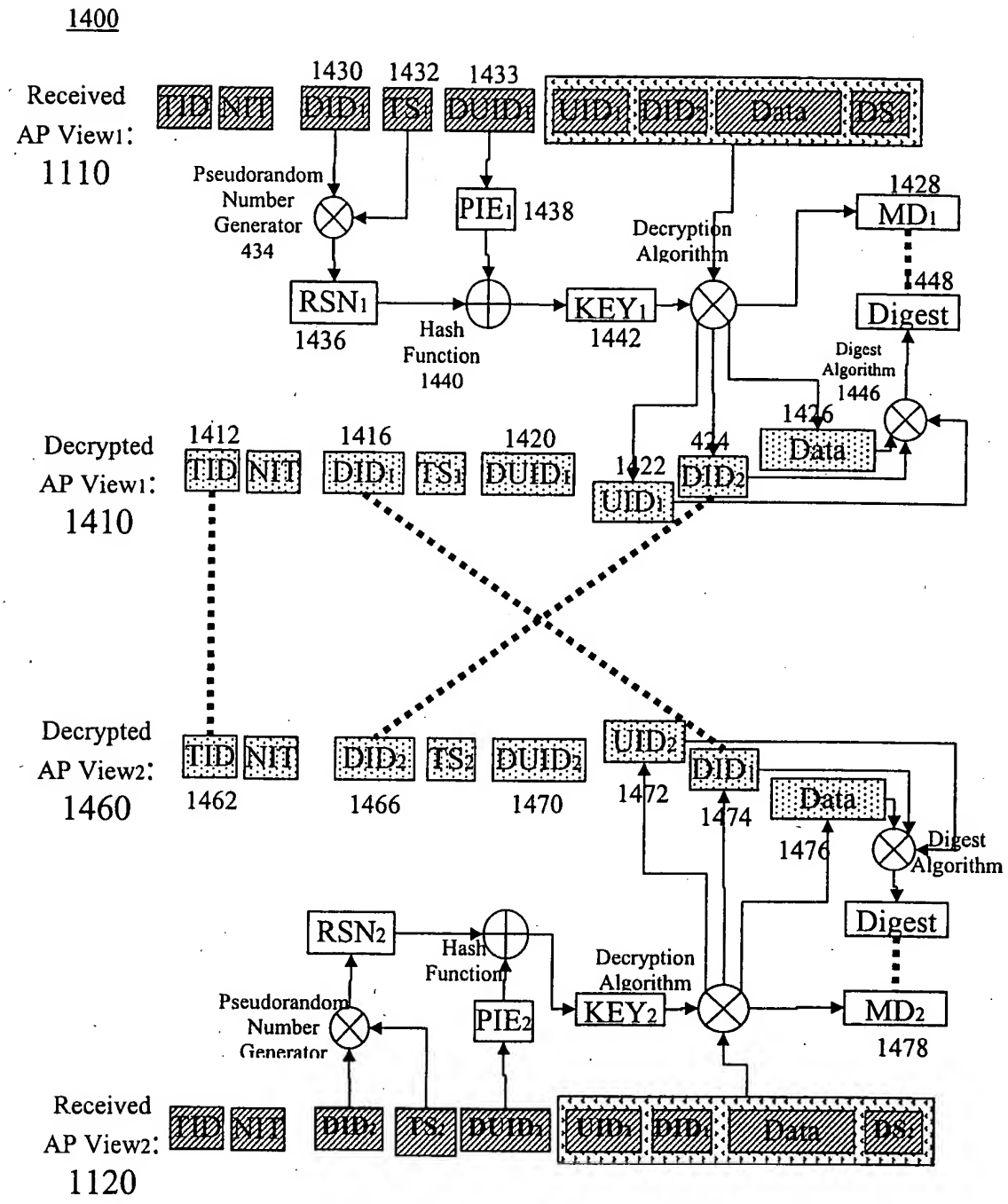

1400
Received AP View1: 1110
TID
NIT
DID1
TS1
DUID1
UID1
DID2
Data
DS1
1430
1432
1433
Pseudorandom Number Generator 434
PIE1
1438
Decryption Algorithm
1428
MD1
RSN1
1436
Hash Function 1440
KEY1
1442
1448
Digest
Digest Algorithm 1446
1426
Decrypted AP View1: 1410
1412
1416
1420
424
1422
Decrypted AP View2: 1460
1462
1466
1470
UID2
DID1
1472
1474
1476
RSN2
Hash Function
Pseudorandom Number Generator
PIE2
KEY2
MD2
1478
Received AP View2: 1120

Figure 60

1500

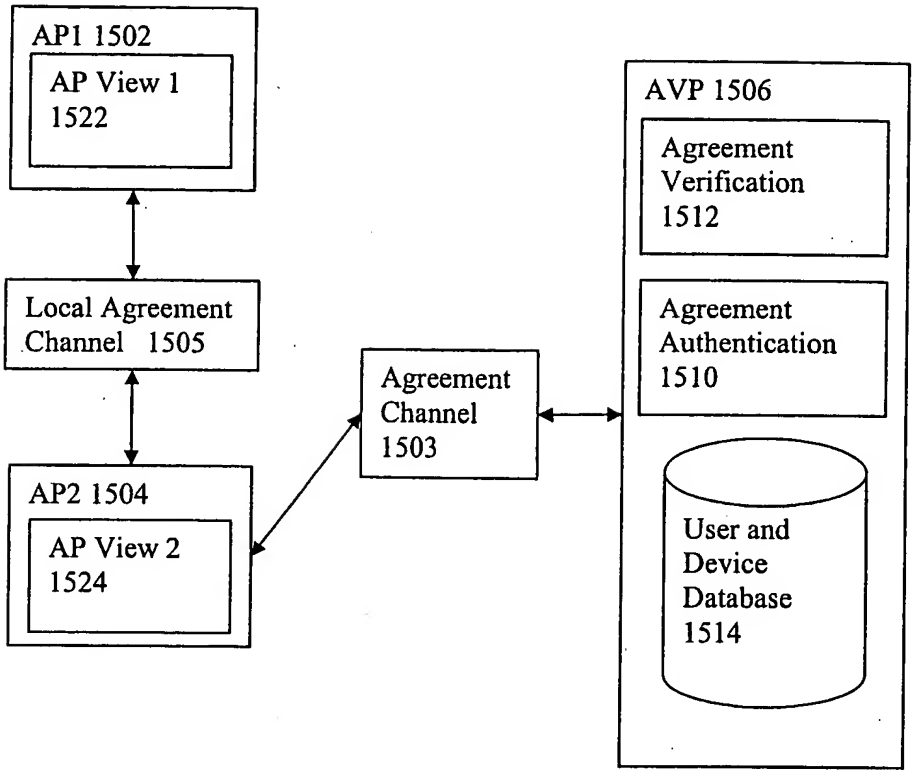


Figure 61

1600

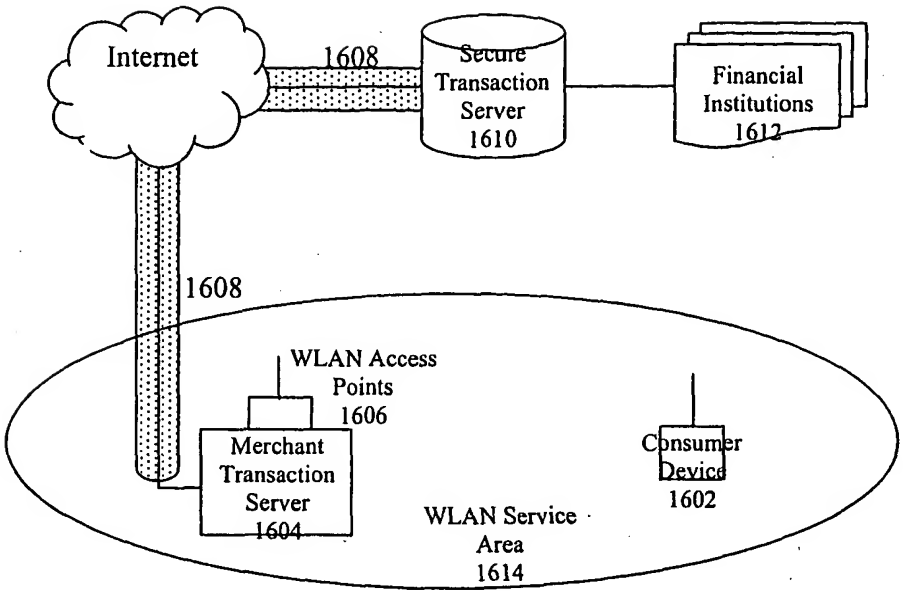


Figure 62

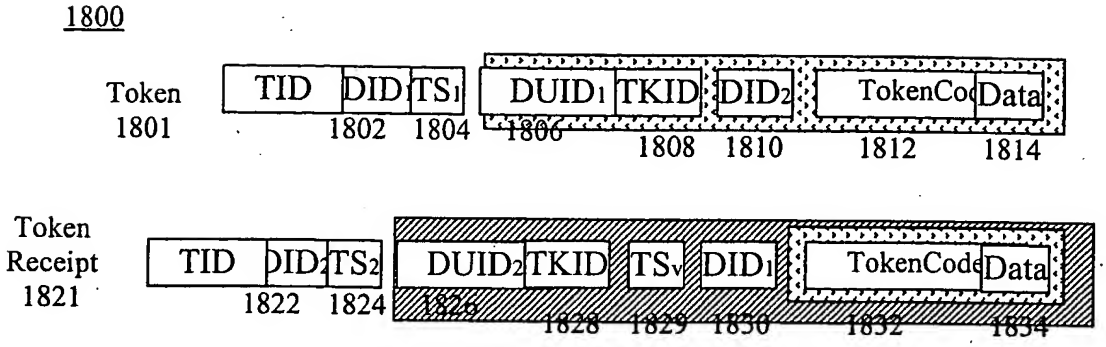

1800
Token
1801
TID
DID1
TS1
DUID1
TKID
DID2
TokenCode
Data
1802
1804
1806
1808
1810
1812
1814
Token
Receipt
1821
TID
DID2
TS2
DUID2
TKID
TSv
DID1
TokenCode
Data
1822
1824
1826
1828
1829
1830
1832
1834

Figure 63